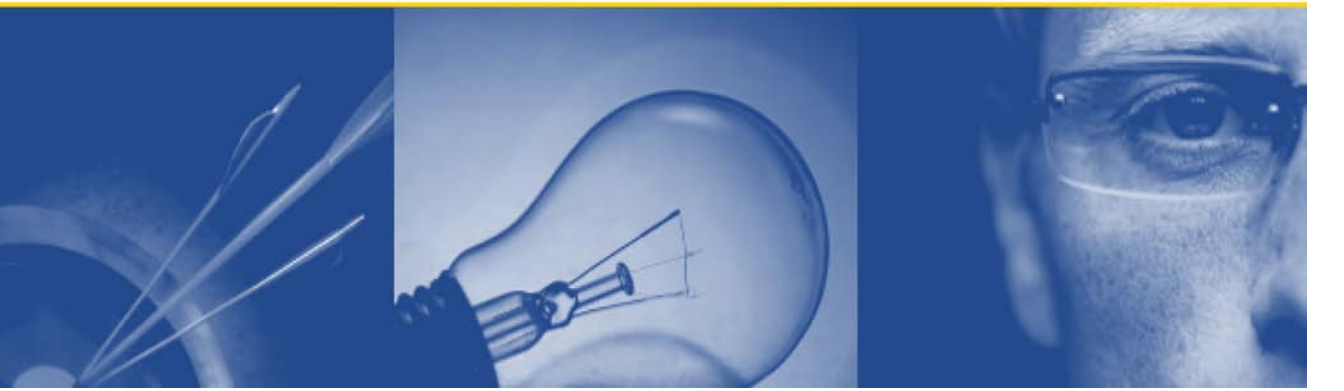
QUEST SOFTWARE

Quest® Group Policy Manager 4.1

Benutzerhandbuch



© 2008 Quest Software, Inc. ALLE RECHTE VORBEHALTEN.

Dieses Handbuch enthält urheberrechtlich geschützte Informationen. Die im vorliegenden Handbuch beschriebene Software unterliegt den Bedingungen der jeweiligen Softwarelizenz oder Geheimhaltungsvereinbarung. Die Software darf nur gemäß den Bedingungen der Vereinbarung benutzt oder kopiert werden. Diese Anleitung darf ohne schriftliche Erlaubnis von Quest Software Inc. weder ganz noch teilweise in beliebiger Form oder durch beliebige elektronische oder mechanische Hilfsmittel einschließlich des Fotokopierens und Speicherns für andere Zwecke als den persönlichen Gebrauch des Käufers vervielfältigt oder weitergegeben werden.

Bei Fragen zur möglichen Verwendung dieser Materialien wenden Sie sich an:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656 USA
www.quest.com
E-Mail: legal@quest.com

Informationen über unsere lokalen und internationalen Büros finden Sie auf unserer Website.

WARENZEICHEN

Quest, Quest Software, das Quest Software-Logo, Aelita, Benchmark Factory, Big Brother, DataFactory, DeployDirector, ERDisk, Fastlane, Final, Foglight, Funnel Web, I/Watch, Imceda, InLook, InTrust, IT Dad, JClass, JProbe, LeccoTech, LiveReorg, NBSpool, NetBase, PerformaSure, PL/Vision, Quest Central, RAPS, SharePlex, Sitraka, SmartAlarm, Speed Change Manager, Speed Coefficient, Spotlight, SQL Firewall, SQL Impact, SQL LiteSpeed, SQL Navigator, SQLab, SQLab Tuner, SQLab Xpert, SQLGuardian, SQLProtector, SQL Watch, Stat, Stat!, Toad, T.O.A.D., Tag and Follow, Vintela, Virtual DBA, und XRT sind Warenzeichen und eingetragene Warenzeichen von Quest Software, Inc. Andere in diesem Handbuch erwähnte Warenzeichen und eingetragene Warenzeichen sind das Eigentum ihrer jeweiligen Besitzer.

Haftungsausschluss

Die Informationen in diesem Dokument werden in Verbindung mit Quest-Produkten zur Verfügung gestellt. Durch dieses Dokument oder den Verkauf eines Quest-Produkts wird keine Lizenz, weder ausdrücklich, implizit, durch Rechtswirkung oder anderweitig, auf jegliches geistiges Eigentum gewährt. MIT AUSNAHME DER BESTIMMUNGEN IN DEN ALLGEMEINEN GESCHÄFTSBEDINGUNGEN VON QUEST, DIE IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT AUFGEFÜHRT SIND, ÜBERNIMMT QUEST KEINERLEI HAFTUNG UND SCHLIESST JEDE EXPLIZITE, IMPLIZITE ODER GESETZLICHE GEWÄHRLEISTUNG FÜR SEINE PRODUKTE AUS, INSBESONDERE DIE IMPLIZITE GEWÄHRLEISTUNG DER MARKTFÄHIGKEIT, DER EIGNUNG ZU EINEM BESTIMMTEN ZWECK UND DIE GEWÄHRLEISTUNG DER NICHTVERLETZUNG VON RECHTEN. UNTER KEINEN UMSTÄNDEN HAFTET QUEST FÜR UNMITTELBARE, MITTELBARE ODER FOLGESCHÄDEN, SCHADENSERSATZ, BESONDERE ODER KONKRETE SCHÄDEN (INSBESONDERE SCHÄDEN, DIE AUS ENTGANGENEN GEWINNEN, GESCHÄFTSUNTER-BRECHUNGEN ODER DATENVERLUSTEN ENTSTEHEN), DIE SICH DURCH DIE NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS ERGEBEN, AUCH WENN QUEST ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE. Quest übernimmt keinerlei Zusicherungen oder Gewährleistung hinsichtlich der Richtigkeit oder Vollständigkeit des Inhalts dieses Dokuments und behält sich das Recht vor, die Angaben und die Produktbeschreibungen jederzeit ohne vorherige Ankündigung zu ändern. Quest übernimmt keine Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Group Policy Manager-Benutzerhandbuch
Aktualisiert - März 2008
Softwareversion - 4.1

INHALT

ÜBER DIESES HANDBUCH 5

ÜBERSICHT 6

FORMATIERUNGSKONVENTIONEN 6

INFO ÜBER QUEST SOFTWARE 7

KONTAKT ZU QUEST SOFTWARE 7

KONTAKT ZUM QUEST-KUNDENDIENST 8

KAPITEL 1
EINFÜHRUNG IN QUEST GROUP POLICY MANAGER 9

QGPM – ÜBERSICHT 10

QGPM – FUNKTIONEN 12

CLIENT/SERVER-ARCHITEKTUR 13

UNTERSTÜTZUNG MEHRERER GESAMTSTRUKTUREN 13

VERSIONSÜBERPRÜFUNG 14

ROLLENBASIERTE DELEGATION 15

ÄNDERUNGSGENEHMIGUNGSVERFAHREN 16

BENACHRICHTIGUNGSSYSTEM 17

GRUPPENRICHTLINIENOBJEKT ACL-EDITOR 17

BERICHTSOPTIONEN 18

VORLAGEN 18

ANGEPASSTE ANSICHTEN 20

OFFLINE GRUPPENRICHTLINIENOBJEKT-TESTS 20

KAPITEL 2
KONFIGURIEREN VON QUEST GROUP POLICY MANAGER 21

KONFIGURIEREN DES VERSIONSÜBERPRÜFUNGSSERVERS 22

FESTLEGEN DER BERECHTIGUNGEN FÜR ADAM 24

ANSCHLUSSANFORDERUNGEN 25

BEARBEITEN DER EIGENSCHAFTEN DES VERSIONSÜBERPRÜFUNGSSERVERS 26

Konfigurieren der rollenbasierten Delegation 28
Erstellen von Rollen 30
Bearbeiten von Rollen 30
Delegieren von Rollen 31
Auswählen von Ereignissen, über die eine Benachrichtigung erfolgen soll 32

Kapitel 3
Verwenden von Quest Group Policy Manager. 33
Verbindung zum Versionsüberprüfungssystem herstellen . .34
Navigieren durch die QGPM-Konsole 35
Benutzereinstellungen konfigurieren. 37
Hinzufügen und Entfernen benutzerdefinierter ADM-Dateien 38
Arbeiten mit der aktiven Umgebung 39
Registrieren von Objekten 39
Registrierter Status 41
Entfernen von registrierten Objekten 44
Arbeiten mit kontrollierten Objekten (Versionsüberprüfungs-Stammcontainer) 44
Erstellen einer benutzerdefinierten Containerhierarchie 45
Auswählen der Sicherheit, der Genehmigungsebenen und der Benachrichtigungsoptionen. 46
Kopieren/Einfügen von Objekten 47
Vorschlagen der Erstellung von kontrollierten Objekten 49
Erstellen von Gruppenrichtlinienobjekten. 49
Erstellen von WMI-Filtern 51
Erstellen von Vorlagen 53
Erstellen von Vorlagen ausgehend von registrierten Gruppenrichtlinienobjekten 54
Arbeiten mit registrierten Objekten. 55
Erstellen von Bezeichnungen 55
Anzeigen des Verlaufs 56
Anzeigen und Bearbeiten von Eigenschaften 57
Anzeigen der Versionsunterschiede 58
Erstellen eines Berichts 58

Arbeiten mit verfügbaren Objekten 59
Ausbuchen von Objekten 60
Anfordern der Löschung eines Objekts 61
Anfordern der Genehmigung 61
Arbeiten mit ausgebuchten Objekten 62
Rückgängig machen einer Ausbuchung 62
Einbuchen kontrollierter Objekte 63
Zurückziehen der Genehmigungsanforderung 64
Wiederherstellen einer vorigen Version 65
Arbeiten mit zur Genehmigung und Bereitstellung anstehenden Objekten 66
Konfigurieren von Genehmigern auf mehreren Ebenen . . 67
Genehmigen und Zurückweisen von Bearbeitungen 68
Planen der Bereitstellung 69
Überprüfen der Konformität 71
Verwenden der Befehlszeilenschnittstelle zur Überprüfung der Konformität 73
Bearbeiten von Objekten 74
Gruppenrichtlinienobjekt bearbeiten 74
Anwenden von Vorlagen 77
Bearbeiten von WMI-Filtern 78
Verknüpfen von Gruppenrichtlinienobjekten 78
Bearbeiten von Vorlagen 80
Importieren der INF-Dateieinstellungen 80
Importieren und Exportieren 81
Exportieren von Objekten 81
Importieren von Objekten 83

KAPITEL 4
BERICHTE ERSTELLEN 85
VERFÜGBARE BERICHTE 86
BERICHTE ÜBER KONTROLLIERTE OBJEKTE 87
DIAGNOSE- UND FEHLERBEHEBUNGSBERICHTE. 90
GRUPPENRICHTLINIENERGEBNISBERICHT 91
BERICHT ÜBER AKTIVE OBJEKTE, DIE ARBEITSKOPIE, DIE AKTUELLESTE VERSION UND UNTERSCHIEDE 93
VERLAUFSBERICHTE. 94
ARBEITEN MIT BERICHTSORDNERN 95

KAPITEL 5
ARBEITEN MIT QUEST ADM-EDITOR. 97
ARBEITEN MIT .ADM-DATEIEN 98
ERSTELLEN UND BEARBEITEN VON .ADM-DATEIEN. 99
MIT DEM ADM-EDITOR ERSTELLTE .ADM-BEISPIELDATEI . . .102
ANPASSEN DER ADM-EDITORANZEIGE 105
GLOSSAR 107
INDEX 111

Über dieses Handbuch

- Übersicht
- Formatierungskonventionen
- Info über Quest Software
- Kontakt zu Quest Software
- Kontakt zum Quest-Kundendienst

Übersicht

Dieses Dokument wurde erstellt, um Sie mit Quest Group Policy Manager, einem Windows Management-Produkt, vertraut zu machen. Das Benutzerhandbuch enthält Informationen, die für die Installation und Verwendung von Quest Group Policy Manager erforderlich sind. Es wurde als Nachschlagwerk für Netzwerkadministratoren, Berater, Analysten und andere IT-Fachleute entwickelt.

Formatierungskonventionen

In diesem Handbuch werden bestimmte Formatierungskonventionen eingehalten, die die effektive Verwendung des Dokuments sicherstellen. Diese Konventionen werden auf unterschiedliche Vorgänge, Symbole, Tastenkombinationen und Querverweise angewandt.

ELEMENT	KONVENTION
Auswählen	Dieses Wort bezieht sich auf Vorgänge wie zum Beispiel das Auswählen oder Markieren diverser Benutzeroberflächenelemente wie Dateien und Optionsfelder.
Fettdruck	In Quest-Produkten angezeigte Benutzeroberflächenelemente, wie zum Beispiel Menüs und Befehle.
Kursivdruck	Wird für Anmerkungen verwendet.
Fetter Kursivdruck	Wird zur Hervorhebung verwendet.
Blaue Schrift	Zeigt einen Querverweis an. Kann in Adobe® Reader® als Hyperlink verwendet werden.
	Wird zum Hervorheben zusätzlicher Informationen verwendet, die für den jeweils beschriebenen Vorgang sachdienlich sind.
	Wird für empfohlene Vorgehensweisen verwendet. Eine empfohlene Vorgehensweise beschreibt detailliert einen Ablauf von Vorgängen, um optimale Ergebnisse zu erzielen.
	Damit werden Vorgänge hervorgehoben, die mit Vorsicht durchzuführen sind.
+	Ein Pluszeichen zwischen zwei Tasten bedeutet, dass beide Tasten gleichzeitig gedrückt werden müssen.
|	Ein senkrechter Strich zwischen zwei Elementen bedeutet, dass diese Elemente in der angegebenen Reihenfolge ausgewählt werden müssen.

Info über Quest Software

Quest Software, Inc., Global Independent Software Vendor Partner of the Year 2007 der Microsoft Corporation, bietet innovative Produkte, die Unternehmen dabei unterstützen, die Leistung und Produktivität ihrer Anwendungen, Datenbanken und Windows-Umgebungen zu steigern. Dank seines tiefgreifenden Know-hows im IT-Bereich und eine permanente Konzentration auf bewährte Verfahren unterstützt Quest weltweit mehr als 50.000 Kunden dabei, die hohen Erwartungen an die Informationstechnologie ihrer Unternehmen zu erfüllen. Die Windows Management-Lösungen von Quest vereinfachen, automatisieren und sichern Active Directory, Exchange Server, SharePoint, SQL Server, .NET und Windows Server und integrieren Unix, Linux und Java in die verwaltete Umgebung. Software von Quest erhalten Sie in den weltweiten Niederlassungen und unter www.quest.com.

Kontakt zu Quest Software

Telefon:	949.754.8000 (Vereinigte Staaten und Kanada)
E-Mail:	info@quest.com
Postanschrift:	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Website:	www.quest.com

Informationen über unsere regionalen und internationalen Büros finden Sie auf unserer Website.

Kontakt zum Quest-Kundendienst

Der Support von Quest ist für Kunden verfügbar, die über eine Evaluierungsversion eines Quest-Produkts verfügen oder die eine kommerzielle Version erworben haben und über einen gültigen Wartungsvertrag verfügen. Quest Support bietet mit SupportLink, unserem Kundendienst im Internet, eine Abdeckung rund um die Uhr. Besuchen Sie SupportLink unter http://support.quest.com/.

Auf der SupportLink-Website haben Sie folgende Möglichkeiten:

- Schnell Tausende von Lösungen finden (Knowledge Base-Artikel und Dokumente)
- Download von Patches und Aktualisierungen
- Anfordern von Hilfe durch einen Support-Techniker
- Protokollieren und Aktualisieren sowie Überprüfung des Status Ihres Supportvorgangs

Im Global Support Guide finden Sie eine ausführliche Erläuterung der Supportprogramme, Onlinedienste, Kontaktinformationen sowie Richtlinien und Vorgehensweisen. Dieses Handbuch ist unter folgender Adresse verfügbar: http://support.quest.com/pdfs/Global Support Guide.pdf.

1

Einführung in Quest Group Policy Manager

- QGPM – Übersicht
- QGPM – Funktionen

QGPM – Übersicht

Die Sicherheit hat für Unternehmen höchste Priorität. Innerhalb von Active Directory sind Gruppenrichtlinienobjekte entscheidend für die Fähigkeit eines Unternehmens, die betriebliche Sicherheit zu gewährleisten. Kernpunkte wie etwa Kennwortrichtlinien, Anmeldezeiten, die Bereitstellung von Software und andere entscheidende Sicherheitseinstellungen werden mittels Gruppenrichtlinienobjekten verwaltet und behandelt. Die Unternehmen benötigen Methoden, um die Einstellungen dieser Gruppenrichtlinienobjekte zu kontrollieren und um Gruppenrichtlinienobjekte auf sinnvolle, sichere und vertrauliche Art und Weise bereitzustellen. Da Gruppenrichtlinienobjekte so wichtig für die ordnungsgemäße Funktionsweise von Active Directory sind, benötigen Unternehmen außerdem Methoden für die Wiederherstellung von Gruppenrichtlinienobjekten, wenn diese falsch aktualisiert wurden oder beschädigt sind.

Quest Group Policy Manager bietet einen Mechanismus zur Kontrolle dieser äußerst wichtigen Komponente von Active Directory. Gruppenrichtlinienobjekte werden auf sichere, dezentrale Weise gesichert und dann einer Versionsüberprüfung unterzogen. Wenn Änderungen vorgenommen werden, wird eine Sicherung des Gruppenrichtlinienobjekts erstellt. Die Änderungen werden über das Versionsüberprüfungssystem verwaltet, und Änderungen erfordern eine Genehmigung. Das gespeicherte Gruppenrichtlinienobjekt kann wiederhergestellt werden, wenn das aktuelle Gruppenrichtlinienobjekt im Verzeichnis aus irgendeinem Grund ungültig ist. Das bedeutet, dass Gruppenrichtlinienobjekte mit einem höheren Maß an Sicherheit verwaltet und bereitgestellt werden können. Bei Auftreten von Problemen wird so die Verzögerungszeit zwischen der Erkennung eines Problems und dessen Lösung durch die Wiederherstellung einer früheren Version des Objekts reduziert.

Als ein Netzwerkadministrator sind Sie für die Gewährleistung des reibungslosen alltäglichen Betriebs des Netzwerks verantwortlich. Diese Tätigkeit umfasst die Verwaltung aller Benutzer- und Computeränderungen sowie die Behebung von Konfigurationsproblemen. Die Implementierung von Gruppenrichtlinienobjekten sollte bei der Planung der Active Directory (AD) -Struktur Ihres Unternehmens berücksichtigt werden.

Sie können Gruppenrichtlinienobjekte verwenden, um spezifische Konfigurationen zu kontrollieren, die über Richtlinieneinstellungen auf Benutzer und Computer angewandt werden. Wenn die Richtlinieneinstellungen zusammengefasst werden, bilden sie ein einziges Gruppenrichtlinienobjekt, das Sie dann auf Sites, Domänen und Organisationseinheiten anwenden können.

Sie können Einstellungen für Benutzer und Computer definieren und sich bezüglich der Umsetzung dieser Richtlinien dann auf das System verlassen. Gruppenrichtlinienobjekte bieten die folgenden Richtlinientypen:

- Computerkonfigurationsrichtlinien wie etwa die Sicherheits- und Anwendungseinstellungen, die angewandt werden, wenn das Betriebssystem initialisiert ist.
- Benutzerkonfigurationsrichtlinien wie etwa Desktop-Einstellungen, Sicherheitseinstellungen, An- und Abmeldeskripts, die angewandt werden, wenn sich Benutzer beim Computer anmelden.
- Registrierungsbasierte Richtlinien wie etwa administrative Vorlagen.

QGPM – Funktionen

Die Gruppenrichtlinienversionsüberprüfung ist von entscheidender Bedeutung für die Bemühungen eines Unternehmens, den kontinuierlichen Betrieb zu gewährleisten. Gruppenrichtlinienobjekte können die Möglichkeiten des Zugriffs eines Benutzers auf das Netzwerk und die Ressourcen, das bzw. die sie für eine effiziente Arbeit benötigen, negativ beeinflussen.

Der Quest Group Policy Manager ermöglicht es den Administratoren, den aktuellen Status eines Gruppenrichtlinienobjekt zu überprüfen, Änderungen in einem gemeinsamen Daten-Repository zu speichern und bei Bedarf einen Bericht über dieses Repository zu generieren. Wenn ein Gruppenrichtlinienobjekt beschädigt ist oder sich nicht mehr in einem betriebsbereiten Zustand befindet, kann jeder vorige Status dieses Gruppenrichtlinienobjekts wiederhergestellt werden.

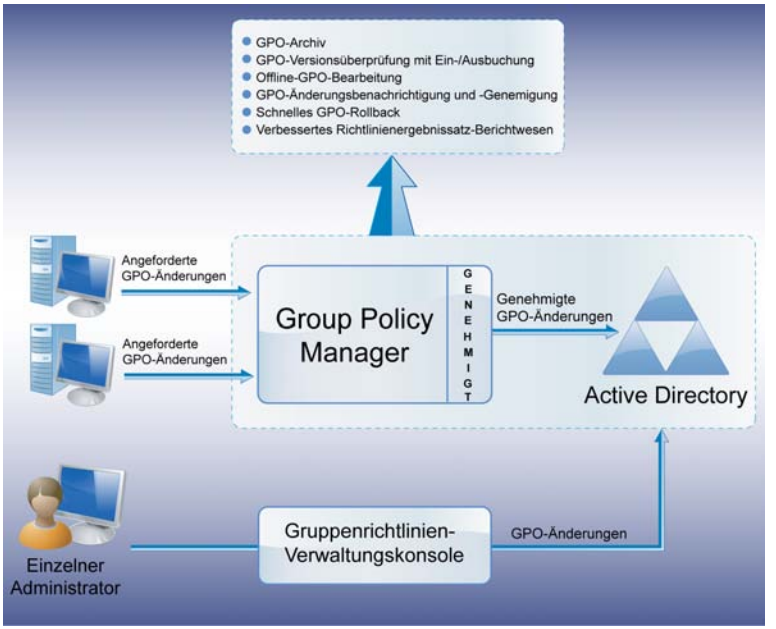


Abbildung 1: Gruppenrichtlinien-Arbeitsablauf

Client/Server-Architektur

Die Client/Server-Architektur erleichtert die granuläre Sicherheit und Delegation. Group Policy Manager wird im Sicherheitskontext eines privilegierten Dienstkontos ausgeführt, das über einen umfassenden Zugriff auf Gruppenrichtlinienobjekte in der verwalteten Gesamtstruktur verfügen muss.

Diese Architektur ermöglicht die Installation mehrerer Server in derselben Gesamtstruktur und bietet somit die Möglichkeit, Domänen unabhängig voneinander zu verwalten. Clients können eine Verbindung zu jedem beliebigen bereitgestellten Server innerhalb jeder beliebigen Active Directory-Gesamtstruktur aufbauen. Group Policy Manager pflegt eine Liste der zuletzt verwendeten Server, zu denen die Benutzer zuletzt eine Verbindung aufgebaut haben, um nachfolgende Serververbindungen zu erleichtern.

Ausführlichere Informationen über die für das Dienstkonto erforderlichen Berechtigungen finden Sie im Handbuch „Quest Group Policy Manager – Erste schritte".

Unterstützung mehrerer Gesamtstrukturen

Die Group Policy Manager 4.1 Verwaltungskonsole ermöglicht Ihnen, mehrere GPM Server-Dienstinstanzen innerhalb derselben Konsole miteinander zu verbinden. Der GPM-Serverdienst kann von einer vertrauenswürdigen oder nicht vertrauenswürdigen Domäne/Gesamtstruktur stammen. Sie haben jetzt die Möglichkeit, die Anmeldeinformationen für alle nicht vertrauenswürdigen Domänen/Gesamtstrukturen anzugeben, wenn Sie eine Verbindung zu nicht vertrauenswürdigen Umgebungen aufbauen. Durch die Auflistung aller GPM Server-Dienstinstanzen haben Sie jetzt die Möglichkeit, auf einfache Art und Weise alle Versionsüberprüfungssysteme ausgehend von einer einzigen Konsole zu verwalten. Dies erleichtert in hohem Maß die Übernahme von Gruppenrichtlinienobjekten aus einer Testumgebung in die Produktion.

Versionsüberprüfung

Die Verknüpfungen mit Gruppenrichtlinienobjekten, WMI-Filtern, Vorlagen und Verwaltungsbereichen (Domänen, Sites und Organisationseinheiten) können in einem geschützten AD-, ADAM- oder SQL-Repository oder in einer Dateifreigabe gespeichert und gesichert werden. Objekte, die im Versionsüberprüfungssystem gespeichert werden, werden mit einer Versionsnummer gekennzeichnet. Sie können dank der Kommentare, die bei jeder vorgenommenen Änderung hinzugefügt werden, und dank der zahlreichen Berichte alle am kontrollierten Objekt vorgenommenen Änderungen anzeigen und zurückverfolgen.

In vorigen Versionen von Group Policy Manager waren Gruppenrichtlinienobjekte, Verknüpfungen und WMI-Filter alle Teil desselben Versionsüberprüfungssystems, wodurch es unmöglich war, Änderungen vor der Bereitstellung granulär zu akzeptieren oder zurückzuweisen. Wenn zum Beispiel Änderungen sowohl den Richtlinieneinstellungen als auch den Verknüpfungen vorgenommen wurden, dann gab es keine Möglichkeit, Änderungen an den Richtlinieneinstellungen anzunehmen und gleichzeitig die vorgeschlagenen Änderungen an den Verknüpfung zurückzuweisen. In Group Policy Manager 4.1 haben Gruppenrichtlinienobjekte, Verwaltungsbereiche und WMI-Filter jetzt ihr eigenes Versionsüberprüfungs-Subsystem, so dass Sie auf granuläre Weise delegieren können, wer Änderungen bearbeiten/erstellen/genehmigen/zurückweisen kann. Jedes dieser Objekte pflegt jetzt seinen eigenen Versions- und Überwachungsverlauf, so dass alle Änderungen (Versionen) separat verfolgt/wiederhergestellt werden können.

Sie können auch benutzerdefinierte Verlaufskommentare (Bezeichnungen) zu Objekten und Containern im Versionsüberprüfungssystem hinzufügen. Diese Funktion ermöglicht es den Benutzern, einen Rollback zu einer durch eine bestimmte Bezeichnung gekennzeichneten Version durchzuführen.

Weitere Informationen finden Sie unter „Verwenden von Quest Group Policy Manager“ auf Seite 33.

Rollenbasierte Delegation

Die Benutzer von Group Policy Manager können Rollen erstellen und definieren, die aus einer Reihe von Rechten für die Ausführung von Vorgängen im Versionsüberprüfungssystem bestehen. Diese Rollen können den Benutzern einen spezifischen Zugang zu den Ressourcen im System verleihen. Group Policy Manager besteht aus den vordefinierten, integrierten Rollen (Benutzer, Moderatoren, Genehmiger, Verknüpfer und Systemadministratoren) und granulären Rechten, die die Benutzer über eine benutzerdefinierte Rolle definieren können.

Zu den benutzerdefinierten Rechten zählen die folgenden Rechte:

- Aus Registrierung entfernen
- Ausbuchen rückgängig machen
- Bereitstellen
- Bezeichnung
- Container bearbeiten
- Container löschen
- Containersicherheit delegieren
- Erstellen/Bearbeiten
- Exportieren
- Genehmigen/Zurückweisen
- Geplante Bereitstellungen abbrechen
- Gruppenrichtlinienobjektvorlage aus INF-Datei importieren
- Konformitätsvorgang
- Lesen
- Löschen
- Registrieren
- Rollback (Konformität)
- Sicherheit delegieren
- Untergeordnete Container erstellen

Durch die Verwendung nativer Active Directory-Sicherheitsmethoden werden die Gruppenrichtlinienobjekte geschützt und sowohl für die Benutzer als auch die Moderatoren delegiert, um die eigenen Methoden des Versionsüberprüfungssystems zu unterstützen.

Weitere Informationen finden Sie unter „Konfigurieren der rollenbasierten Delegation“ auf Seite 28.

Änderungsgenehmigungsverfahren

Alle im Versionsüberprüfungssystem durchgeführten Änderungen werden erst dann in die Online-Active Directory (AD) -Umgebung übernommen, wenn sie von speziell zugeordneten Benutzern genehmigt und bereitgestellt wurden.

Sie können ein Verfahren zur parallelen Genehmigung auf Container/Objektebene erzwingen, so dass alle an der aktiven Produktionsumgebung vorgenommenen Änderungen von allen festgelegten Genehmigern sorgfältig geprüft und genehmigt werden müssen.

Das Ziel der parallelen Genehmigung mehrerer Änderungen besteht darin, es zu ermöglichen, dass der Genehmigungsprozess auf der kombinierten Zustimmung von mehreren Genehmigern anstelle von einem einzigen Genehmiger beruht. So erhalten die Kunden ein noch höheres Maß an Sicherheit, weil sie sich jetzt darauf verlassen können, dass ihre Arbeit nicht durch einen einzigen bösartig gesonnenen Genehmiger ruiniert werden kann.

Die Bereitstellung von Änderungen innerhalb des Systems ist ein kritischer Prozess, der Auswirkungen auf die aktive Umgebung hat. Um die Auswirkungen der Unterbrechung zu minimieren, sollte dieses Verfahren während eines Zeitraums ausgeführt werden, in dem die Auswirkungen auf die Benutzer minimal sind, da die Änderungen am Gruppenrichtlinienobjekt das Verhalten bestimmter Systeme verändern können.

Um das Auftreten möglicher Probleme zu vermeiden, können Sie die Bereitstellung der Änderungen zu einem bestimmten Datum und zu einer bestimmten Uhrzeit planen, das bzw. die Ihren Bedürfnissen am besten entspricht.

Weitere Informationen finden Sie unter „Planen der Bereitstellung“ auf Seite 69.

Benachrichtigungssystem

Ein umfassendes Benachrichtigungssystem, das es den Benutzern ermöglicht, eine Vielzahl von Versionsüberprüfungsereignissen zu kontrollieren und sofort Details per E-Mail zu empfangen.

Benutzer können den Benachrichtigungsdienst abonnieren/abbestellen. Dieser Dienst basiert auf einem granulär definierten Ereignistrigger wie etwa: Registrieren/Aus Registrierung entfernen, Einbuchen/Ausbuchen, Erstellen/Löschen/Ändern von Genehmigungsanforderungen, Genehmigung/Zurückweisung der Erstellung/des Löschens/der Änderung von Anforderungen, Konformität (Gelöscht, Rollback, Integrieren in aktive Umgebung), administrative Rückgängigmachung der Ausbuchung eines anderen Benutzers, Verknüpfen/Verknüpfung aufheben und Erstellen/Löschen/Bearbeiten eines Containers.

Berichte werden in die Benachrichtigungs-E-Mails aufgenommen, wenn mehr Details erforderlich sind. So enthalten zum Beispiel Einbuchungsbenachrichtigungen einen Einstellungsbericht (um die Einstellungen anzuzeigen, die gerade eingebucht wurden) und einen Unterschiedsbericht (um die Unterschiede zwischen dieser Version und der letzten Version anzuzeigen).

Weitere Informationen finden Sie unter „Auswählen von Ereignissen, über die eine Benachrichtigung erfolgen soll“ auf Seite 32.

Gruppenrichtlinienobjekt ACL-Editor

Eine Sicherheitsgruppe, ein Benutzer oder ein Computer muss sowohl über die Berechtigung zum Lesen als auch zum Anwenden einer Gruppenrichtlinie verfügen, um eine Richtlinie anwenden zu können. Standardmäßig verfügen alle Benutzer und Computer über diese Berechtigungen für alle neuen Gruppenrichtlinienobjekte. Sie erben diese Berechtigungen über ihre Mitgliedschaft in der Gruppe „Authentifizierte Benutzer“. In Group Policy Manager 4.1 können Sie zusätzlich zur Änderung des Sicherheitsfilters auch die Berechtigungen einer bestimmten Gruppe verwalten. Wenn Sie zum Beispiel nicht möchten, dass ein Gruppenrichtlinienobjekt auf eine Gruppe von Benutzern angewandt wird, können Sie auf einfache Weise die Berechtigung für ein bestimmtes Gruppenrichtlinienobjekt so konfigurieren („Anwenden der Gruppenrichtlinie verweigern“), dass sie nicht auf die Gruppe von Benutzern angewandt wird.

Weitere Informationen finden Sie unter „Arbeiten mit Quest ADM-Editor“ auf Seite 97.

Berichtsoptionen

Echtzeit und historische Berichte

Sie können Berichtsvorlagen für schnelle Echtzeit-Berichterstellungszwecke sowie einfache Status-Quo-Berichte für historische Zwecke generieren. Diese Funktion ermöglicht eine schnelle Wiederherstellung von aktuellen Daten aus den Echtzeit-Berichtsvorlagen. All diese Berichte werden jetzt asynchron erstellt; daher müssen Sie nicht mehr länger warten, bis ein Bericht generiert wurde, bevor Sie die Erstellung eines neuen Berichts starten können.

Weitere Informationen über die Berichtsoption finden Sie unter „Berichte erstellen“ auf Seite 85.

Vorlagen

Als Administrator möchten Sie gewährleisten, dass Gruppenrichtlinieneinstellungen für Ihre Gruppenrichtlinienobjekte richtig eingegeben werden und den Standards Ihres Unternehmens entsprechen. Da sich die Standards Ihrer Organisationen ändern, müssen Sie Ihre Gruppenrichtlinienobjekte überprüfen und die erforderlichen Änderungen an den Einstellungen vornehmen.

Durch die Verwendung von Vorlagen können Sie die Verwaltung von Gruppenrichtlinien vereinfachen, indem Sie einmalig Gruppenrichtlinienobjektvorlagen erstellen und dann zur Wiederverwendung verteilen. Dieser Mechanismus gewährleistet, dass die Gruppenrichtlinieneinstellungen der Gruppenrichtlinienobjekte in Ihrem Unternehmen konsistent sind.

Vorlagen sind eine Zusammenfassung von Richtlinieneinstellungen, die Sie auf vorhandene Gruppenrichtlinienobjekte anwenden oder für die Erstellung neuer Gruppenrichtlinienobjekte verwenden können. Sie können in anderen Domänen, untergeordneten Domänen oder Domänen in einer anderen Gesamtstruktur wiederverwendet werden. Sie können auch im gesamten Unternehmen angefangen von zentralen Administratoren bis hin zu den lokalen Administratoren in Zweigniederlassungen verteilt werden. Die Administratoren können ähnliche Gruppenrichtlinienobjekte auf der Grundlage der Vorlagen oder neue Gruppenrichtlinienobjekte, die einer Unternehmensrichtlinie entsprechen, erstellen.

Vorlagen können die folgenden Einstellungen umfassen:

- Computerkonfigurationseinstellungen wie etwa die Sicherheits- und Anwendungseinstellungen, die angewandt werden, wenn das Betriebssystem initialisiert ist.
- Benutzerkonfigurationseinstellungen wie etwa Desktop-Einstellungen, Sicherheitseinstellungen, An- und Abmeldeskripts, die angewandt werden, wenn sich Benutzer beim Computer anmelden.
- Registrierungsbasierte Einstellungen wie etwa administrative Vorlagen.

Vorlagen können nur auf registrierte Gruppenrichtlinienobjekte innerhalb des Versionsüberprüfungssystems angewandt werden. Die an einem Gruppenrichtlinienobjekt auf der Grundlage von Vorlageneinstellungen vorgenommenen Änderungen müssen denselben Genehmigungsprozess durchlaufen wie alle anderen an den Gruppenrichtlinienobjekten im System vorgenommenen Änderungen. Weitere Informationen finden Sie unter „Arbeiten mit zur Genehmigung und Bereitstellung anstehenden Objekten“ auf Seite 66.

Der Quest ADM-Editor ist in QGPM enthalten, um Sie bei der Erstellung und Bearbeitung von ADM-Dateien über eine benutzerfreundliche Schnittstelle zu unterstützen. Die ADM-Dateien können dann in das Versionsüberprüfungssystem importiert und von den Vorlagen verwendet werden.

Weitere Informationen finden Sie unter „Arbeiten mit Quest ADM-Editor“ auf Seite 97.

Angepasste Ansichten

Sie können kontrollierte Objekte in einer benutzerdefinierten Containerhierarchie organisieren. Jeder Container verfügt über seinen eigenen Sicherheitsdeskriptor, in dem den Trustees Rollen für die Definition des Zugriffs auf den Container, untergeordneten Container oder einfach auf ein bestimmtes Gruppenrichtlinien-objekt in diesen Containern zugewiesen (delegiert) werden können.

„Versionsüberprüfungs-Root-Hierarchie" sollte als eine Methode zur Organisation von vielen Objekten in einer logischen, auf der Unternehmensstruktur basierenden Ansicht für die Administratorverwaltung verwendet werden.

Die Suchordner ermöglichen Ihnen, schnell kontrollierte Objekte auf der Grundlage ihres Zustands innerhalb des Versionsüberprüfungssystems anzuzeigen. „Ordner suchen" sollte als eine einfache Methode zur Anzeige des Status von Objekten innerhalb des Versionsüberprüfungssystems für die Benutzerverwaltung verwendet werden.

Weitere Informationen finden Sie unter „Erstellen einer benutzerdefinierten Containerhierarchie" auf Seite 45.

Offline Gruppenrichtlinienobjekt-Tests

Mit Hilfe des Exportassistenten können Sie Gruppenrichtlinienobjekte vor deren Implementierung offline testen. Weitere Informationen finden Sie unter „Arbeiten mit verfügbaren Objekten" auf Seite 59.

2

Konfigurieren von Quest Group Policy Manager

- Konfigurieren des Versionsüberprüfungsservers
- Festlegen der Berechtigungen für ADAM
- Anschlussanforderungen
- Bearbeiten der Eigenschaften des Versionsüberprüfungsservers
- Konfigurieren der rollenbasierten Delegation
- Auswählen von Ereignissen, über die eine Benachrichtigung erfolgen soll

Konfigurieren des Versionsüberprüfungsservers

Sie müssen den Versionsüberprüfungsserver konfigurieren, wenn Sie erstmalig eine Verbindung zu ihm herstellen.

Gehen Sie folgendermaßen vor, um den Versionsüberprüfungsserver zu konfigurieren:

1. Klicken Sie mit der rechten Maustaste auf den Knoten „Quest Group Policy Manager" und wählen Sie **Verbinden mit**.
2. Wählen Sie den Versionsüberprüfungsserver, zu dem Sie eine Verbindung herstellen möchten, und klicken Sie dann auf **OK**.
3. Wählen Sie Active Directory oder ADAM als Ihren Speicherort und klicken Sie dann auf **Weiter**.
4. Wenn Sie Active Directory auswählen, wählen Sie einen Domänen-controller (DC) als Versionsüberprüfungsserver aus und klicken Sie dann auf **Weiter**.

   Jeder beliebige DC in jeder beliebigen Domäne der ausgewählten Gesamtstruktur kann als Versionsüberprüfungsmaster ausgewählt werden. Den Versionsüberprüfungsmaster können Sie sich als eine weitere FSMO-Rolle im Microsoft-Sinne vorstellen (wie etwa der Schemamaster, der PDC-Emulator und der RID-Master).

   Group Policy Manager ist eine verzeichnisfähige Anwendung, und all ihre Anwendungsinformationen werden im Konfigurationscontainer von Active Directory gespeichert. Daher werden alle Informationen automatisch auf alle anderen DCs repliziert. Der Versionsüber-prüfungsmaster ist jedoch die verbindliche Quelle für alle erforderlichen Versionsüberprüfungsvorgänge. Wenn dieser Master in den Offline-Status übergeht, dann sind die Benutzer nicht mehr in der Lage, Vorgänge wie etwa das Einbuchen einer erforderlichen Gruppenrichtlinienobjektänderung durchzuführen, bis das Problem beseitigt wurde.
5. Geben Sie die Server-Anmeldeinformationen, die Authentifizierungs-methode und die Anschlussinformationen ein und klicken Sie auf **Weiter**.

Der Benutzername/Port/Server (jedoch nicht das Kennwort) werden zwischengespeichert, so dass Sie diese Informationen beim nächsten Öffnen der Konsole nicht erneut eingeben müssen.

6. Wählen Sie, wo Sie die historischen Sicherungsinformationen speichern möchten.

   Sicherungen können im Lauf der Zeit eine beträchtliche Größe erreichen. Die Speicherung dieser Sicherungen in AD ist in einigen Unternehmensumgebungen möglicherweise nicht die optimale Konfiguration.

   Sie haben die Möglichkeit, AD, den Active Directory Application Mode (ADAM), SQL Server/MSDE 2000 oder eine Netzwerkfreigabe auszuwählen.

OPTION	BEI AUSWAHL DIESER OPTION:
Active Directory	Klicken Sie auf **Weiter**.
ADAM	Geben Sie den Server und den Anschlussnamen ein und klicken Sie auf **Weiter**. Weitere Informationen über eine ADAM-Installation finden Sie unter „Festlegen der Berechtigungen für ADAM“ auf Seite 24.
SQL Server/MSDE	Geben Sie den Servernamen und die erforderlichen Authentifizierungsinformationen ein und klicken Sie dann auf **Weiter**. Hinweis: Wenn der Server als eine einzige Instanz installiert wird, muss er als ein Servername/Instanzname und nicht als der SQL-Servername angegeben werden.
Netzwerkfreigabe	Wählen Sie die entsprechende Netzwerkfreigabe oder das entsprechende Verzeichnis aus und klicken Sie dann auf **Weiter**.

Ein automatisierter SMTP-Benachrichtigungsmechanismus warnt festgelegte Benutzer per E-Mail, dass eine ausstehende Anforderung oder eine Reihe von ausstehenden Anforderungen bereit für die Bearbeitung sind.

7. Klicken Sie erforderlichenfalls auf **SMTP-Benachrichtigung aktivieren**, geben Sie den Server und den Port ein und klicken Sie dann auf **Weiter**. Geben Sie die E-Mail-Spezifikationen ein und klicken Sie auf **Weiter**.

   – ODER –

   Klicken Sie auf **Weiter**.

8. Wählen Sie, welche Benutzer das Recht haben werden, eine Verbindung zum Versionsüberprüfungsserver herzustellen und diesen zu verwalten, und klicken Sie dann auf **Weiter**.
9. Klicken Sie auf **Fertig stellen**.

   Jetzt, da das System konfiguriert ist, können die Benutzer eine Verbindung zur Versionsüberprüfung aufbauen und die entsprechenden Funktionen nutzen.

Benutzer mit den entsprechenden Rechten können die Servereinstellungen jederzeit konfigurieren, indem sie mit der rechten Maustaste auf den Knoten „Quest Group Policy Manager" klicken und „Servereigenschaften" auswählen.

Festlegen der Berechtigungen für ADAM

Um Group Policy Manager mit einer ADAM-Installation nutzen zu können, muss den Benutzern die Administratorrolle zugewiesen werden.

Gehen Sie folgendermaßen vor, um die Berechtigungen für ADAM festlegen:

1. Öffnen Sie ADAM ADSI-Edit (ADSI-Edit wird als Teil der ADAM-Tools installiert).
2. Stellen Sie eine Verbindung zum Konfigurationsbenennungskontext her und suchen Sie dann den Container „Rollen".
3. Um die Benutzerrechte zu vergeben, klicken Sie mit der rechten Maustaste auf die Rolle **Administratoren** und wählen Sie dann **Eigenschaften**.
4. Suchen Sie das Attribut „Mitglieder" und klicken Sie auf **Bearbeiten**.
5. Fügen Sie das Dienstkonto zur ausgewählten Rolle hinzu.

Erforderlichenfalls können Sie das ADAM-Supporttool „dsacls" verwenden, um die von diesen Rollen gewährten Rechte detaillierter zu definieren oder um den Benutzern bestimmte Rechte zu gewähren.

Anschlussanforderungen

Führen Sie vor dem Öffnen dieser Dienste für ein nicht vertrauenswürdiges Netzwerk eine sorgfältige Analyse durch.

Die folgenden Ports müssen geöffnet werden, um den korrekten Betrieb der Anwendung zu gewährleisten:

Eine Namensauflösung kann durch Verwendung des DNS an Port 53 oder des WINS (Downlevel) an Port 137 erreicht werden.

Zwischen dem Client und dem QGPM-Server:

Port 40200 (Standard)

Um den Versionsüberprüfungsserver an einem benutzerdefinierten Port in 4.1 auszuführen, müssen Sie den folgenden Registrierungswert konfigurieren:

Schlüssel: HKLM/Software/Quest Software/Quest Group Policy Manager/ Remoting
Wertname: Port
Werttyp: DWord
Gültige Werte: 1-65536

Wenn dieser Wert nicht konfiguriert ist, wird der Standardwert (Port 40200) verwendet.

Vom Quest Group Policy Manager-Server:

Konfigurationsspeicher

- LDAP-Dienst - TCP/UDP - 389 -oder- ADAM-Port (Standard bis 389 oder 50000)

Gruppenrichtlinienobjektarchive

- Wenn Sie eine Netzwerkfreigabe für die Gruppenrichtlinienobjekt-Sicherungsspeicherung verwenden, müssen die folgenden Ports geöffnet werden: 135, 136, 138, 139 und/oder 445.
- Wenn Sie SQL Server für den Gruppenrichtlinienobjekt-Sicherungsspeicher verwenden, müssen die entsprechenden Ports geöffnet werden. Der Standard-Port von SQL Server ist 1433 oder 1533, wenn die Option „Server verbergen" aktiviert ist.
- Wenn Sie Named Pipes mit SQL verwenden, werden beliebige Ports benötigt. SQL Named Pipes ist keine empfohlene Konfiguration über Firewalls.
- Wenn Sie ADAM für die Gruppenrichtlinienobjekt-Sicherungs-speicherung oder Konfigurationsdaten verwenden, wählt ADAM als Standardeinstellung Port 389, wenn ADAM nicht gemeinsam mit AD genutzt wird. Ist AD bereits installiert, wählt ADAM standardmäßig den Port 50000.

Bearbeiten der Eigenschaften des Versionsüberprüfungsservers

Benutzer, denen der Zugriff gewährt wurde, können auf die Eigenschaften des Versionsüberprüfungsservers zugreifen und bei Bedarf ändern. Zu diesen Eigenschaften zählen unter anderem der Verzeichnisserver, wo die Gruppenrichtlinienobjektsicherungen gespeichert sind, die für die Definition der Sicherheit im System verwendeten Rollen, die SMTP-Einstellungen und der Zugriff für die Bearbeitung dieser Einstellungen sowie Protokollierungs- und Lizenzierungsoptionen.

Gehen Sie folgendermaßen vor, um die Konfiguration des Versionsüberprüfungsservers zu bearbeiten:

1. Klicken Sie mit der rechten Maustaste auf die Domäne, wählen Sie **Eigenschaften** und wählen Sie dann die erforderlichen Serveroptionen aus.
2. Wählen Sie die Registerkarte **Zugriff**, um Benutzer hinzuzufügen und zu entfernen, die auf die Serveroptionen zugreifen und diese ändern können.

   Hier können Sie auch Benutzer hinzufügen und entfernen, die nur auf den Versionsüberprüfungsserver zugreifen können.

3. Wählen Sie die Registerkarte **Speicher** aus, um die gewünschten Speicheroptionen zu ändern (Active Directory, ADAM, SQL oder gemeinsam genutzter Ordner).
4. Wählen Sie die Registerkarte **Rollen** aus, um Rollen zu erstellen und zu bearbeiten, die verwendet werden, um die Rechte für das Versionsüberprüfungssystem zu delegieren.

   Die integrierten Rollen werden angezeigt. Die zu jeder Rolle gehörenden Berechtigungen können durch Auswahl der Rolle und Anklicken der Schaltfläche Rolle bearbeiten angezeigt werden. Vordefinierte Rollen können nicht geändert werden.

   Weitere Informationen über die Erstellung und das Delegieren von Rollen finden Sie unter „Konfigurieren der rollenbasierten Delegation" auf Seite 28.
5. Wählen Sie die Registerkarte **SMTP**, um die globalen SMTP-Benachrichtigungsoptionen zu ändern.

Benutzer können die E-Mail-Adresse für ihre Benachrichtigungs-E-Mail in ihren persönlichen Einstellungen ändern. Weitere Informationen „Benutzereinstellungen konfigurieren" auf Seite 37.

6. Klicken Sie auf die Registerkarte **Protokollierung** und wählen Sie den Speicherort der Protokolldatei und den Typ der zurück-zuverfolgenden Informationen aus.

   Sie können wählen, die Daten im Ereignisprotokoll oder in einem bestimmten Verzeichnis, in dem die Protokolldateien erstellt werden, zu protokollieren oder gar keine Protokollierung durchzuführen.

   Außerdem können Sie die zu protokollierenden Ereignistypen auswählen. Nachfolgend sind die Ereignistypen aufgeführt: Dienstvorgänge (wie etwa der Start und Stopp von Diensten), Benutzervorgänge (wie etwa Einbuchen, Genehmigen, Bearbeiten), Fehler und Debug-Informationen (werden vom Personal des Quest-Supports verwendet).
7. Klicken Sie auf die Registerkarte **Lizenz**, um die aktuellen Lizenzinformationen anzuzeigen.

   – ODER –

   Wählen Sie die Option **Lizenz aktualisieren**, wechseln Sie zum Speicherort der neuen Lizenz und klicken Sie dann auf **OK**.
8. Wenn Sie alle erforderlichen Optionen ausgewählt haben, klicken Sie auf **OK**.

Konfigurieren der rollenbasierten Delegation

Benutzer von Group Policy Manager, die die Berechtigung zum Ändern der Servereigenschaften haben, können Rollen erstellen, die bestimmte Benutzer (die mit der Sicherheitsrolle „Delegieren") nutzen können, um zu kontrollieren, wer bestimmte Funktionen im Versionsüberprüfungssystem ausführen kann. Weitere Informationen über Benutzer mit der Berechtigung zur Erstellung von Rollen finden Sie unter „Konfigurieren des Versionsüberprüfungsservers" auf Seite 22.

Group Policy Manager umfasst die folgenden vordefinierten Rollen:

ROLLE	IN DER ROLLE ENTHALTENE RECHTE
Systemadministrator	Systemadministratoren können jeden beliebigen Vorgang im Versionsüberprüfungssystem durchführen: • Genehmigen/Zurückweisen • Geplante Bereitstellungen abbrechen • Konformitätsvorgang • Erstellen/Bearbeiten • Untergeordnete Container erstellen • Containersicherheit delegieren • Sicherheit delegieren • Löschen • Container löschen • Bereitstellen • Container bearbeiten • Exportieren • Gruppenrichtlinienobjektvorlage aus INF importieren • Bezeichnung • Lesen • Registrieren • Rollback (Konformität) • Ausbuchen rückgängig machen • Aus Registrierung entfernen

ROLLE	IN DER ROLLE ENTHALTENE RECHTE
Moderator	Moderatoren können jeden Vorgang durchführen, den ein Benutzer durchführen kann, und zusätzlich Ausbuchungen von anderen Benutzern rückgängig machen und den Konformitätsassistenten ausführen. Sie können außerdem folgende Vorgänge ausführen: • Erstellen/Bearbeiten • Löschen • Ausbuchungen anderer Benutzer rückgängig machen • Exportieren • Lesen
Benutzer	Benutzer können alle grundlegenden Vorgänge des Versionsüberprüfungssystems wie etwa Einbuchen, Ausbuchen, Bearbeiten, Vorlagen übernehmen etc. ausführen. Sie können außerdem folgende Vorgänge ausführen: • Erstellen/Bearbeiten • Löschen • Exportieren • Lesen
Genehmiger	Genehmiger können an Gruppenrichtlinienobjekten ausstehende Vorgänge genehmigen oder zurückweisen. Wenn Sie außerdem über die Berechtigung zum Bereitstellen eines Gruppenrichtlinienobjekts verfügen, können Sie auch die Aktualisierungen im Unternehmen bereitstellen.

Die vordefinierten Rollen können nicht geändert werden.

Erstellen von Rollen

Sie können auf einfache Weise neue Rollen mit jedem der individualisierten Rechten erstellen:

Gehen Sie folgendermaßen vor, um eine neue Rolle zu erstellen:

1. Klicken Sie mit der rechten Maustaste auf die Domäne und wählen Sie **Eigenschaften**.
2. Wählen Sie die Registerkarte **Rollen**.
3. Klicken Sie auf **Neue Rolle hinzufügen**.
4. Geben Sie einen Namen und eine Beschreibung für die Rolle ein und klicken Sie auf **Weiter**.
5. Wählen Sie die Rechte aus, die Sie in die Rolle aufnehmen möchten, und klicken Sie dann auf **Fertig stellen**.

Bearbeiten von Rollen

Gehen Sie folgendermaßen vor, um Rollen zu bearbeiten:

1. Klicken Sie mit der rechten Maustaste auf die Domäne und wählen Sie **Eigenschaften**.
2. Wählen Sie die Registerkarte **Rollen**.
3. Wählen Sie die Rolle, die Sie bearbeiten möchten, und klicken Sie auf **Rolle bearbeiten**.
4. Nehmen Sie die gewünschte Änderungen vor und klicken Sie auf **OK**.
5. Klicken Sie erneut auf **OK**, um die Änderungen anzuwenden.

Delegieren von Rollen

Wenn die entsprechenden Rollen eingerichtet sind, können Benutzer mit der Rolle „Sicherheit delegieren" beginnen, die Sicherheit über Container und Gruppenrichtlinienobjekte an bestimmte Benutzer und Gruppen zu delegieren.

Gehen Sie folgendermaßen vor, um Rechte bezüglich des Versionsüberprüfungssystems mit Hilfe von Rollen zu delegieren:

1. Klicken Sie mit der rechten Maustaste auf den Versionsüberprüfungs-Stammknoten, den erforderlichen Container oder das erforderliche Objekt und wählen Sie **Eigenschaften**.
2. Wählen Sie die Registerkarte **Sicherheit**.
3. Klicken Sie auf **Hinzufügen**, um die Benutzer und Gruppen auszuwählen, auf die Sie die Rolle anwenden möchten.
4. Wählen Sie die Rolle, die Sie anwenden möchten, und klicken Sie auf **OK**.

   Die angegebenen Benutzer haben nun die in der zugewiesenen Rolle enthaltenen Rechte über den ausgewählten Container oder das ausgewählte Objekt.

Auswählen von Ereignissen, über die eine Benachrichtigung erfolgen soll

Mit Hilfe der Benachrichtigungsoption können Sie ein System einrichten, bei dem Sie jedes Mal, wenn ein bestimmter Vorgang innerhalb des Versionsüberprüfungssystems ausgeführt wird, eine E-Mail empfangen.

Gehen Sie folgendermaßen vor, um eine Benachrichtigung einrichten:

1. Klicken Sie mit der rechten Maustaste auf das Objekt, für das Sie eine Benachrichtigung einrichten möchten, und wählen Sie dann **Eigenschaften**.
2. Wählen Sie die Registerkarte **Benachrichtigungen**.
3. Wählen Sie die Ereignisse aus, über die Sie benachrichtigt werden möchten, und klicken Sie dann auf **OK**.

   Wenn die angegebenen Ereignisse am ausgewählten Objekt (und im Fall eines Containers darüber hinaus) eintreten, wird eine Benachrichtigungs-E-Mail gesendet.

Informationen über das Festlegen der E-Mail-Adresse für die Benachrichtigungsmeldungen finden Sie unter „Benutzereinstellungen konfigurieren“ auf Seite 37

3

Verwenden von Quest Group Policy Manager

- Verbindung zum Versionsüberprüfungs-system herstellen
- Navigieren durch die QGPM-Konsole
- Benutzereinstellungen konfigurieren
- Arbeiten mit der aktiven Umgebung
- Registrieren von Objekten
- Arbeiten mit kontrollierten Objekten (Versionsüberprüfungs-Stammcontainer)
- Erstellen einer benutzerdefinierten Containerhierarchie
- Vorschlagen der Erstellung von kontrollierten Objekten
- Arbeiten mit registrierten Objekten
- Arbeiten mit verfügbaren Objekten
- Arbeiten mit ausgebuchten Objekten
- Arbeiten mit zur Genehmigung und Bereitstellung anstehenden Objekten
- Überprüfen der Konformität
- Einbuchen kontrollierter Objekte
- Importieren und Exportieren

Verbindung zum Versions-überprüfungssystem herstellen

Wenn die Anwendung vom Administrator vollständig konfiguriert wurde (siehe „Konfigurieren des Versionsüberprüfungsservers“ auf Seite 22), können die Benutzer eine Verbindung zum Versionsüberprüfungssystem herstellen.

Gehen Sie folgendermaßen vor, um eine Verbindung zum Versionsüberprüfungssystem herzustellen:

1. Klicken Sie mit der rechten Maustaste auf den Knoten „Quest Group Policy Manager“ und wählen Sie **Verbinden mit**.
2. Wählen Sie einen vorhandenen Versionsüberprüfungsserver aus, zu dem Sie eine Verbindung herstellen möchten, und klicken Sie dann auf **OK**.

   – ODER –

   Klicken Sie auf **Neu**, um eine neue Verbindung zu erstellen.

Navigieren durch die QGPM-Konsole

Die QGPM-Konsole besteht aus einem Fenster, das in drei Bereiche unterteilt ist:

- Im linken Fensterbereich wird die Konsolenstrukturansicht angezeigt. Die Konsolenstruktur ist eine hierarchische Struktur, die in einer Konsole verfügbare Elemente (Knoten) anzeigt. Ausgehend von der Konsolenstruktur können Sie die aktiven Unternehmensobjekte und die Versionsüberprüfungssysteme anzeigen, die für Sie verfügbar sind.
- Der mittlere Bereich enthält das Detailfenster. Das Detailfenster zeigt Informationen und Funktionen an, die zu dem in der Konsolenstruktur ausgewählten Element gehören.
- Der rechte Bereich ist das Fenster „Aktionen". Das Fenster „Aktionen" enthält alle Vorgänge, die ausgehend von den in der Konsolenstruktur und im Detailfenster ausgewählten Knoten und Objekten verfügbar sind.
- Die Suchordner ermöglichen Ihnen, schnell kontrollierte Objekte auf der Grundlage ihres Zustands innerhalb des Versionsüberprüfungs-systems anzuzeigen.

  Es werden nur die Objekte angezeigt, für die Sie Leserechte haben. Der Ordner Für mich ausgebucht zeigt alle Objekte an, die Sie aktuell ausgebucht haben, so dass Sie gewährleisten können, dass bei Durchführung eines Massen-Einbuchungsvorgangs keine erforderlichen Aktualisierungen vergessen werden.

  „Ordner suchen" sollte als eine einfache Methode zur Anzeige des Status von Objekten innerhalb des Versionsüberprüfungssystems für die Benutzerverwaltung verwendet werden.

  „Versionsüberprüfungs-Root-Hierarchie" sollte als eine Methode zur Organisation von vielen Objekten in einer logischen, auf der Unternehmensstruktur basierenden Ansicht für die Administrator-verwaltung verwendet werden.

- Der Container „Fundsachen" enthält Objekte, die sich innerhalb eines aus dem Knoten „Versionsüberprüfungs-Root" gelöschten Untercontainers befunden haben. Ausgehend von diesem Container können Sie die Objekteigenschaften anzeigen, das Objekt in den Versionsüberprüfungs-Stammcontainer oder einen Untercontainer verschieben und das Objekt aus der Registrierung entfernen.

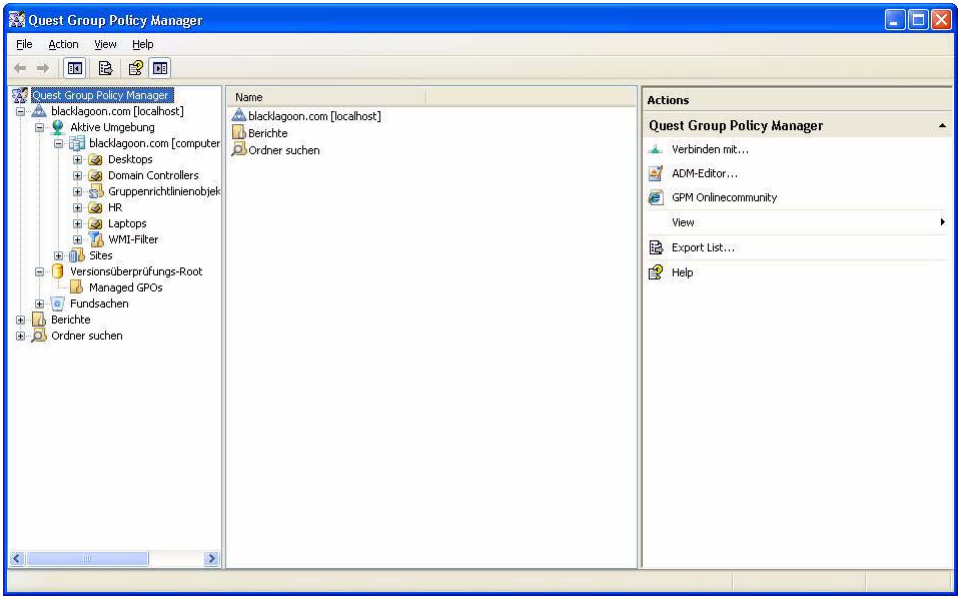
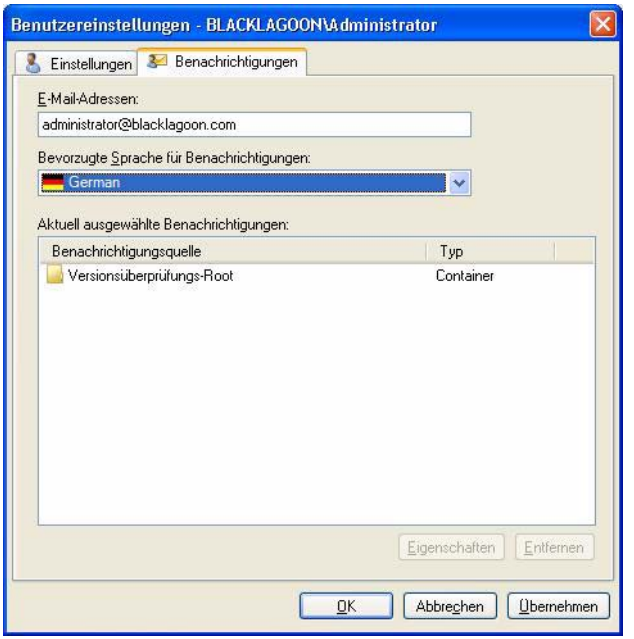


Abbildung 1: QGPM-Konsole

Benutzereinstellungen konfigurieren

Gehen Sie folgendermaßen vor, um die benutzerdefinierten Einstellungen zu konfigurieren:

1. Klicken Sie mit der rechten Maustaste auf den Server und wählen Sie **Benutzereinstellungen**.
2. Wählen Sie auf der Registerkarte **Einstellungen** einen Ordner oder ein Laufwerk, in bzw. auf dem Ihre Berichte gespeichert werden sollen.
3. Wählen Sie die Registerkarte **Benachrichtigungen** und geben Sie die E-Mail-Adresse ein, an die die Benachrichtigungsmeldungen gesendet werden sollen.
4. Um Ihre aktuellen Benachrichtigungsabonnements anzuzeigen und zu bearbeiten, wählen Sie die Benachrichtigungsquelle und klicken Sie dann auf die Schaltfläche **Eigenschaften**, um die zugehörigen Vorgänge anzuzeigen.



5. Um eine Benachrichtigung zu entfernen, wählen Sie die Benachrichtigungsquelle und klicken Sie dann auf die Schaltfläche **Entfernen**.
6. Klicken Sie auf **OK**.

Hinzufügen und Entfernen benutzerdefinierter ADM-Dateien

Sie können jede beliebige benutzerdefinierte .adm-Datei hinzufügen, um Einstellungen hinzuzufügen, die Sie auf Gruppenrichtlinienobjekte und Vorlagen anwenden können. So können Sie beispielsweise auswählen, Office 2000.adm-Dateien hinzuzufügen, die es Ihnen ermöglichen, die vielen verfügbaren Einstellungen zu steuern und zu konfigurieren.

Alle in Quest Group Policy Manager-Vorlagen verwendeten ADM-Dateien müssen dem Unicode-Format entsprechen.

Gehen Sie folgendermaßen vor, um benutzerdefinierte ADM-Dateien hinzuzufügen:

1. Erweitern Sie Quest Group Policy Manager, klicken Sie mit der rechten Maustaste auf den Serverknoten und wählen Sie dann **ADM hinzufügen/entfernen**.
2. Fügen Sie neue .adm-Dateien hinzu, indem Sie auf **Hinzufügen** klicken.
3. Wählen Sie die entsprechende .adm-Datei aus und klicken Sie auf **Öffnen**.
4. Klicken Sie auf **OK**.

   Wenn Sie eine Vorlage erstellen, enthält der Ordner „Administrative Vorlagen" die Einstellungen aus der .adm-Datei.

Gehen Sie folgendermaßen vor, um benutzerdefinierte ADM-Dateien zu entfernen:

1. Erweitern Sie Quest Group Policy Manager, klicken Sie mit der rechten Maustaste auf den Serverknoten und wählen Sie dann **ADM hinzufügen/entfernen**.
2. Entfernen Sie .adm-Dateien, indem Sie auf **Entfernen** klicken.
3. Klicken Sie auf **OK**.

Arbeiten mit der aktiven Umgebung

- Registrieren von Objekten
- Registrierter Status
- Entfernen von registrierten Objekten

Registrieren von Objekten

Um die Arbeit mit dem Versionsüberprüfungssystem starten zu können, müssen die Gruppenrichtlinienobjekte, WMI-Filter und Verwaltungsbereiche (Sites, Domänen und Organisationseinheiten) registriert sein.

Nur Benutzer mit der Berechtigung zum Registrieren/zum Entfernen aus der Registrierung können Objekte registrieren und aus der Registrierung entfernen.

Wenn ein Objekt erstmalig zum System hinzugefügt wird, wird es automatisch im Verlauf des Versionsüberprüfungssystems gesichert (gespeichert) und mit der Version 1.0 gekennzeichnet, wenn während des Registrierungsverfahrens keine andere, höhere Versionsnummer angegeben wird.

QGPM arbeitet mit bereits vorhandenen Gruppenrichtlinienobjekten, WMI-Filtern und Verwaltungsbereichen sowie jeder beliebigen Vorlage oder jeden beliebigen anderen, vom System erstellten Objekten.

Versionsnummernvergabe: Immer, wenn eine Änderung vorgenommen wurde (Objekt eingebucht), wird die Stelle hinter dem Dezimalpunkt der Versionsnummer inkrementiert. Beispiel: v1.2, v1.3 und v1.4.
Wenn von einem Benutzer mit der entsprechenden Rolle eine Änderung auf das Unternehmen angewandt wird, wird die Stelle vor dem Dezimalpunkt der Versionsnummer inkrementiert. Beispiel: v2.0 und v3.0.

Gehen Sie folgendermaßen vor, um Objekte zu registrieren:

1. Erweitern Sie Quest Group Policy Manager und die Aktive Umgebung und wählen Sie das Objekt, das Sie beim Versionsüberprüfungssystem registrieren möchten.
2. Klicken Sie mit der rechten Maustaste und wählen Sie dann **Registrieren**.
3. Wählen Sie den Container aus, in dem Sie das registrierte Objekt speichern möchten, und klicken Sie auf **OK**.

   Sobald die Objekte registriert wurden, befinden sie sich im auswählten Container unter dem Stammverzeichnis der Versionsüberprüfung; ihre Versionsnummer wird dabei anfänglich auf 1.0 gesetzt. Sie können jetzt ausgebucht und bearbeitet werden.

   Sobald Objekte registriert sind, können Benutzer mit den delegierten Rechten registrierte Gruppenrichtlinienobjekte mit einem Verwaltungsbereich (Sites, Domänen und Organisationseinheiten) verknüpfen. Weitere Informationen finden Sie unter „Verknüpfen von Gruppenrichtlinienobjekten“ auf Seite 78.

   Wenn Sie von einem vorhandenen Versionsüberprüfungssystem zu einem anderen System migrieren, können Sie die Stelle vor dem Dezimalpunkt der Versionsnummer in jede beliebige Zahl größer als 1.0 ändern.

Registrierter Status

Sie können den Status von registrierten Gruppenrichtlinienobjekten, WMI-Filtern, Vorlagen, Sites, Domänen und Organisationseinheiten auf einfache Weise anzeigen. Die Objekte sind entweder zum Ausbuchen verfügbar, bereits ausgebucht oder eingebucht und warten auf die Genehmigung, um für das Unternehmen bereitgestellt zu werden. Die in jeder Phase für Sie verfügbaren Optionen hängen von Ihrer spezifischen Rolle und Ihren Berechtigungen ab.

Registrierte Objekte haben einen der folgenden Zustände:

STATUS	BEFINDET SICH DAS GRUPPEN-RICHTLINIENOBJEKT IN DIESEM STATUS, HABEN SIE JE NACH ZUGEWIESENER ROLLE FOLGENDE MÖGLICHKEITEN:
Verfügbar	• Objekte ausbuchen • Objekte bearbeiten • Gruppenrichtlinienobjekt importieren und exportieren • Vorlagen erstellen und übernehmen • Konformität prüfen • Benachrichtigung senden, dass die Änderungen bereit für die Genehmigung sind (für Objekte, die über eine Versionsnummer mit einer Zahl größer als Null hinter dem Dezimalpunkt verfügen) • Verlauf anzeigen • Unterschied zwischen zwei Gruppen-richtlinienobjekten oder Verwaltungs-bereichen anzeigen • Berichte über aktive Gruppen-richtlinienobjekte, Offline-Objekte und die Unterschiede zwischen diesen Objekten erstellen und speichern • Objekteigenschaften bearbeiten • Objekte aus der Registrierung entfernen • Objekte zum Löschen markieren

STATUS	BEFINDET SICH DAS GRUPPEN-RICHTLINIENOBJEKT IN DIESEM STATUS, HABEN SIE JE NACH ZUGEWIESENER ROLLE FOLGENDE MÖGLICHKEITEN:
Ausgebucht	• Jegliche Ausbuchungen rückgängig machen • Objekte bearbeiten • Gruppenrichtlinienobjekt importieren und exportieren • Gruppenrichtlinienobjekte mit Verwaltungsbereichen verknüpfen • Objekte einbuchen • Einbuchen und Genehmigung anfordern • Objekteigenschaften bearbeiten • Verlauf anzeigen • Unterschied zwischen zwei Objekten anzeigen • Berichte über aktive Gruppen-richtlinienobjekte, Offline-Objekte und die Unterschiede zwischen diesen Objekten erstellen und speichern • Vorlagen erstellen und übernehmen • Konformität prüfen • Änderungen genehmigen

STATUS	BEFINDET SICH DAS GRUPPEN-RICHTLINIENOBJEKT IN DIESEM STATUS, HABEN SIE JE NACH ZUGEWIESENER ROLLE FOLGENDE MÖGLICHKEITEN:
Anstehende Genehmigung	• Änderungen genehmigen und zurückweisen • Genehmigung zurückziehen • Änderungen für die Umgebung bereitstellen • Konformität prüfen • Verlauf anzeigen • Objekteigenschaften bearbeiten • Berichte über aktive Gruppen-richtlinienobjekte, Offline-Gruppen-richtlinienobjekte und die Unterschiede zwischen diesen Gruppenrichtlinien-objekten erstellen und speichern • Gruppenrichtlinienobjekteinstellungen exportieren
Anstehende Bereitstellung	• Änderungen für die Umgebung bereitstellen • Genehmigung zurückziehen

Entfernen von registrierten Objekten

Wenn das Objekte nicht länger für Änderungen verfügbar sein soll, können Sie es aus dem Versionsüberprüfungssystem entfernen, wenn Sie über die Berechtigung zum Entfernen aus der Registrierung verfügen.

Gehen Sie folgendermaßen vor, um Objekte aus dem Versions-überprüfungssystem zu entfernen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie dann **Erweitert | Aus Registrierung entfernen**.

Arbeiten mit kontrollierten Objekten (Versionsüberprüfungs-Stammcontainer)

- Erstellen einer benutzerdefinierten Containerhierarchie
- Auswählen der Sicherheit, der Genehmigungsebenen und der Benachrichtigungsoptionen
- Kopieren/Einfügen von Objekten
- Arbeiten mit registrierten Objekten
- Arbeiten mit verfügbaren Objekten
- Arbeiten mit ausgebuchten Objekten
- Arbeiten mit zur Genehmigung und Bereitstellung anstehenden Objekten

Erstellen einer benutzerdefinierten Containerhierarchie

Sie können registrierte Objekte in einer benutzerdefinierten Hierarchie unter dem Versionsüberprüfungs-Stammcontainer organisieren.

Jeder Container verfügt über seinen eigenen „Sicherheitsdeskriptor", in dem Trustees Rollen zugewiesen werden können, um deren Zugriff auf das Objekt festzulegen. Weitere Informationen finden Sie unter „Konfigurieren der rollenbasierten Delegation" auf Seite 28.

Nach der Erstellung der Container können Sie Objekte leicht in andere Container innerhalb derselben Domäne verschieben bzw. dorthin kopieren.

Gehen Sie folgendermaßen vor, um einen neuen Container zu erstellen:

1. Erweitern Sie die Strukturansicht und wählen Sie den Versions-überprüfungs-Root oder einen Untercontainer aus.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Neu | Container**.
3. Geben Sie den Containernamen ein und klicken Sie dann auf **OK**.

Gehen Sie folgendermaßen vor, um einen Container zu löschen:

1. Erweitern Sie die Strukturansicht und suchen Sie den Container unter dem Knoten „Versionsüberprüfungs-Root".
2. Klicken Sie mit der rechten Maustaste auf den Container und wählen Sie **Löschen**.

Gehen Sie folgendermaßen vor, um einen Container mit einer Bezeichnung zu versehen:

1. Erweitern Sie die Strukturansicht und suchen Sie den erforderlich Container unter dem Knoten „Versionsüberprüfungs-Root".
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Bezeichnung**.
3. Geben Sie die Bezeichnung für den Container ein und klicken Sie auf **OK**.

   Wenn Sie den Container und die Option „Verlauf anzeigen" auswählen, haben Sie die Möglichkeit, die Bezeichnung in die Anzeige mit aufzunehmen. Weitere Informationen finden Sie unter „Erstellen von Bezeichnungen" auf Seite 55.

Auswählen der Sicherheit, der Genehmigungsebenen und der Benachrichtigungsoptionen

Sie haben die Möglichkeit, Schutzeinrichtungen zu implementieren, indem Sie Genehmiger auf mehreren Ebenen benennen. Bei Auswahl dieser Option muss eine Änderung von der angegebenen Anzahl von Genehmigern genehmigt werden, bevor sie für die Bereitstellung in der aktiven Umgebung verfügbar ist.

Gehen Sie folgendermaßen vor, um die Sicherheit, die Genehmigungsebene und die Benachrichtigungsoptionen für einen Container festzulegen:

- Klicken Sie mit der rechten Maustaste auf den Versionsüberprüfungs-Stammknoten, den erforderlichen Container oder das erforderliche Objekt und wählen Sie **Eigenschaften**.

  Hier können Sie mittels der Sicherheitsoptionen die Verantwortung über den Container delegieren, die Genehmigungsebenen konfigurieren und auf der Registerkarte „Benachrichtigung" die Ereignisse festlegen, über die eine Benachrichtigung erfolgen soll. Weitere Informationen über das Delegieren von Rollen, finden Sie unter „Konfigurieren der rollenbasierten Delegation" auf Seite 28. Weitere Informationen über das Benachrichtigungssystem, finden Sie unter „Auswählen von Ereignissen, über die eine Benachrichtigung erfolgen soll" auf Seite 32.

Kopieren/Einfügen von Objekten

Objekte können innerhalb der Hierarchie auf einfache Weise kopiert und eingefügt werden. Wenn Sie das Gruppenrichtlinienobjekt innerhalb eines Versionsüberprüfungssystems einfügen, haben Sie die Möglichkeit, den Gruppenrichtlinienobjektverlauf beizubehalten.

Es können mehrere Objekte ausgeschnitten und eingefügt werden, aber Sie können nur jeweils ein Objekt kopieren und einfügen.

Sie können jetzt die Version des zu kopierenden Objekts auswählen und müssen nicht mehr die neueste Version auswählen (oder die Arbeitskopie, falls verfügbar, wie dies der Fall in der Version 3.1 war). Wenn ein einzelnes Objekt eingefügt wird, haben Sie die Option, die aktive Version (falls verfügbar), die Arbeitskopie (wenn das Objekt aktuell für Sie ausgebucht ist) oder jede beliebige historische Version des zu kopierenden Objekts auszuwählen.

Sie können keine Objekte von einem Server zum anderen oder von einer Gesamtstruktur zur anderen kopieren oder verschieben (Ausschneiden/Einfügen). Wenn Objekte in einem Server/in einer Gesamtstruktur ausgeschnitten und dann in einem anderen Server/in einer anderen Gesamtstruktur eingefügt werden, wird das ausgeschnittene Objekt beim Einfügen zu einer Kopie des ausgeschnittenen Objekts. In diesem Fall gelten alle normalen Kopier-/Einfügeregeln.

Wenn Sie das Objekt einfügen, wird es ein neues Objekt mit der Versionsnummer 0.0 im Status „Ausgebucht". Diese Versionsnummer gibt an, dass die Version erst dann als „Aktiv" betrachtet wird, wenn das Objekt das Genehmigungsverfahren durchlaufen hat. Wenn Sie das Gruppenrichtlinienobjekt mit dem Verlauf kopieren und einfügen, wird es zu einem Gruppenrichtlinienobjekt, das mit dem Original-Gruppenrichtlinienobjekt gemeinsam genutzt wird.

Wenn Sie ein ausgebuchtes Objekt kopieren und einfügen, werden Änderungen an der Arbeitskopie nicht eingefügt. Nur der Verlauf bis zur zuletzt ausgebuchten Version kann eingefügt werden.

Wenn Sie ein Objekt zwischen Containern im selben Dienst per Drag & Drop verschieben, wird der Vorgang „Verschieben" gestartet. Wenn Sie es zwischen Containern in verschiedenen Diensten per Drag & Drop verschieben, wird der Vorgang „Kopieren" ausgeführt.

Wenn Sie mit der rechten Maustaste klicken und das Objekt dann per Drag & Drop verschieben, haben Sie zwei Optionen: „Hierher kopieren" und „Hierher verschieben". Wenn Sie das Objekt zwischen Containern im selben Dienst verschieben, bedeutet „Kopie" ein Kopiervorgang und „Verschieben" ein „Verschiebevorgang". Wenn Sie das Objekt jedoch zwischen Containern in verschiedenen Diensten per Drag & Drop verschieben, wird unabhängig von der ausgewählten Option ein Kopiervorgang ausgeführt.

Gehen Sie folgendermaßen vor, um ein Objekt zu kopieren und einzufügen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf ein Objekt und wählen Sie **Kopieren**.
3. Klicken Sie mit der rechten Maustaste auf den Zielcontainer und wählen Sie **Einfügen**.
4. Wählen Sie ausgehend vom Exportassistenten die Version, die Sie testen möchten, und klicken Sie dann auf **Weiter**.
5. Wählen Sie die Versionsüberprüfungs-Zieldomäne für das Objekt aus und klicken Sie dann auf **Weiter**.

   Wenn Sie den Verlauf aus der Quelle kopieren, können Sie den Verlauf der am eingefügten Objekt vorgenommenen Änderungen anzeigen, wobei die Vorgänge eindeutig als an der Quelle ausgeführte Vorgänge markiert sind.

   Wenn ein Objekt mit demselben Namen bereits im Zielcontainer vorhanden ist, haben Sie die folgenden Optionen: Abbrechen des Einfügevorgangs, Umbenennen oder Fortsetzen mittels des doppelt vorhandenen Namens.
6. Wählen Sie (falls erforderlich) eine Migrationstabelle aus und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**.

Vorschlagen der Erstellung von kontrollierten Objekten

- Erstellen von Gruppenrichtlinienobjekten
- Erstellen von WMI-Filtern
- Erstellen von Vorlagen
- Erstellen von Vorlagen ausgehend von registrierten Gruppenrichtlinienobjekten

Erstellen von Gruppenrichtlinienobjekten

Benutzer mit der entsprechenden Berechtigung können die Erstellung eines Gruppenrichtlinienobjekts, das aktuell nicht in der Unternehmensumgebung vorhanden ist, sowie dessen Aufnahme in das Versionsüberprüfungssystem vorschlagen. Es können jedoch nur Benutzer, die über die Berechtigung zur Bereitstellung verfügen, die Änderungen auf das aktive Unternehmen anwenden.

Zunächst ist das Gruppenrichtlinienobjekt nicht mit irgendeinem Verwaltungsbereich innerhalb der aktiven Unternehmensumgebung verknüpft. Wenn die Erstellung des Gruppenrichtlinienobjekts genehmigt ist, können Sie Verknüpfungen hinzufügen. Weitere Informationen finden Sie unter „Verknüpfen von Gruppenrichtlinienobjekten“ auf Seite 78.

Sie können auch das Hinzufügen eines Gruppenrichtlinienobjekts aus einer Vorlage anfordern. Weitere Informationen finden Sie unter „Importieren der INF-Dateieinstellungen“ auf Seite 80.

Die manuelle Erstellung eines neuen Gruppenrichtlinienobjekts kann zeitaufwendig sein. Die Erstellung eines Gruppenrichtlinienobjekts auf der Grundlage einer zuvor erstellten Vorlage vereinfacht dieses Verfahren.

Die Erstellung eines Gruppenrichtlinienobjekts auf der Grundlage einer Vorlage ist auch nützlich, wenn die Vorlage für die Erstellung mehrerer Gruppenrichtlinienobjekte mit einer Reihe gemeinsamer Einstellungen verwendet wird. Wenn das Gruppenrichtlinienobjekt auf dieser Grundlage erstellt worden ist, kann jedes Gruppenrichtlinienobjekt so angepasst werden, dass es spezifischen Bedürfnissen entspricht.

Wenn Sie ein neues Gruppenrichtlinienobjekt erstellen, haben Sie die Möglichkeit, eine oder mehrere Vorlagen auf dieses Gruppenrichtlinienobjekt anzuwenden.

Überprüfen auf in Konflikt stehende Vorlageneinstellungen

Group Policy Manager führt eine Überprüfung auf in Konflikt stehende Vorlageneinstellungen durch, wenn Sie ein neues Gruppenrichtlinienobjekt erstellen und Vorlagen auf dieses Objekt anwenden oder wenn Sie ein Gruppenrichtlinienobjekt auswählen, das bereits erstellt wurde, und eine Vorlage auf dieses Objekt anwenden. Wenn zwei oder mehr Vorlagen ausgewählt sind, wird ein Dialogfeld geöffnet, und Sie haben die Möglichkeit, die Überprüfung auf Konflikte zu überspringen.

Wenn Konflikte festgestellt werden, können Sie den Vorgang fortsetzen, wobei die Einstellungen der letzten Vorlage Vorrang haben. Sie können die Details der in Konflikt stehenden Einstellungen anzeigen, indem Sie auf die Schaltfläche „Details" klicken. Hierdurch wird der Vorlagenkonfliktbericht angezeigt.

Gehen Sie folgendermaßen vor, um die Erstellung eines Gruppenrichtlinienobjekts vorzuschlagen:

1. Erweitern Sie den Versionsüberprüfungs-Root-Knoten, klicken Sie mit der rechten Maustaste auf den erforderlichen Container und wählen Sie dann **Neu | Gruppenrichtlinienobjekt**.
2. Geben Sie einen Namen ein, wählen Sie den Speicherort für das Gruppenrichtlinienobjekt aus und klicken Sie dann auf **Weiter**.
3. Wählen Sie erforderlichenfalls die auf das Gruppenrichtlinienobjekt anzuwendenden Vorlagen aus.
4. Klicken Sie auf **Editor starten**.
5. Nehmen Sie die erforderlichen Bearbeitungen am neuen Gruppenrichtlinienobjekt vor und schließen Sie den Gruppenrichtlinienobjekt-Editor.
6. Wählen Sie die Einstellungen, die Sie in das Gruppenrichtlinienobjekt aufnehmen möchten, und klicken Sie dann auf **Weiter**.
7. Klicken Sie erforderlichenfalls auf **Hinzufügen**, geben Sie Sicherheitsfilter ein und klicken Sie dann auf **Weiter**.
8. Wählen Sie erforderlichenfalls die anzuwendenden WMI-Filter und klicken Sie dann auf **Weiter**.
9. Klicken Sie auf **Fertig stellen**.

   Wenn Sie Bearbeitungen vornehmen und das Gruppenrichtlinienobjekt einbuchen, wird die Version auf Version 0.1 aktualisiert. Diese Zahl wird um .1 erhöht, bis Sie die Vorgänge „Einbuchen" und „Genehmigung anfordern" ausführen. An diesem Punkt ist das Gruppenrichtlinienobjekt nicht aktiv.

Wenn Sie Ihre Bearbeitungen abgeschlossen haben, können Sie die Vorgänge „Einbuchen" und „Genehmigung anfordern" ausführen. Wenn das Gruppenrichtlinienobjekt eingebucht und die Genehmigung angefordert ist, wird das neue Gruppenrichtlinienobjekt automatisch registriert und ist mit der Version 1.0 verfügbar.

Objekte der Version 0.0 sind noch nicht im System aktiv.

Die Ausbuchung von Objekten der Version 0.0 kann von einem anderen Benutzer mit der Berechtigung zur Rückgängigmachung der Ausbuchung rückgängig gemacht werden. Dies führt zum Löschen des Objekts aus dem System und zum Löschen der Arbeitskopie.

Objekte der Version 0.0, für die eine Genehmigung ansteht, sind nur für den Benutzer, der das Objekt erstellt hat, und für Benutzer mit der Berechtigung zur Genehmigung sichtbar.

Die Konformität wird für Objekte der Version 0.0 nicht überprüft.

Erstellen von WMI-Filtern

Mit Hilfe der Windows Management Instrumentation (WMI) -Filter können Sie steuern, wo Gruppenrichtlinienobjekte auf der Grundlage der Attribute des Zielcomputers angewandt werden.

Sie können WMI-Filter insbesondere verwenden, um festzulegen, auf welche Zielcomputer das Gruppenrichtlinienobjekt auf der Grundlage einer im Filter vorhandenen Abfrage angewandt wird. Die Abfrage im WMI-Filter, die mit einem Gruppenrichtlinienobjekt verknüpft ist, wird im Zielcomputer ausgewertet.

So kann Ihr Filter beispielsweise „Computer auswählen, die eine Prozessorgeschwindigkeit von mehr als 2 GHz haben" lauten. Wenn der Zielcomputer den Kriterien entspricht, wird das Gruppenrichtlinienobjekt angewandt. Falls nicht, wird das Gruppenrichtlinienobjekt nicht angewandt.

Der WMI-Filter und das Gruppenrichtlinienobjekt, mit dem er verknüpft ist, müssen sich in derselben Domäne befinden.

WMI-Filter werden nur von Windows XP, Windows Server 2003 und höher unterstützt.

Gehen Sie folgendermaßen vor, um die Erstellung eines WMI-Filters vorzuschlagen:

1. Erweitern Sie den Container „Versionsüberprüfung", in dem Sie den neuen WMI-Filter speichern möchten.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Neu | WMI-Filter**.
3. Geben Sie einen Namen für den neuen WMI-Filter ein.
4. Wählen Sie eine Domäne, in der der WMI-Filter erstellt werden soll, fügen Sie erforderlichenfalls eine Beschreibung hinzu und klicken Sie dann auf **Weiter**.
5. Wählen Sie einen Namespace (Standard: Stammverzeichnis\CIMv2) und geben Sie eine gültige WQL (Windows Query Language) - Zeichenkette in das Feld „Abfrage" ein.

   Es muss mindestens eine Abfrage mit einem WMI-Filter verbunden sein, um den Vorgang fortsetzen zu können.

Weitere Informationen über das Schreiben von WQL-Abfragen finden Sie in der Microsoft Documentation.

6. Um eine zusätzliche Abfrage zum Filter hinzuzufügen, wählen Sie **Neue Abfrage** und geben Sie den Root-Namespace und die Abfrage wie in Schritt 5 beschrieben ein.
7. Um eine Abfrage zu löschen, klicken Sie auf die Schaltfläche „x" neben der Abfrage in der Liste.
8. Klicken Sie auf **Fertig stellen**.

   Der WMI-Filter wird in den Status „Ausstehende Erstellung" gesetzt und muss von einem Benutzer mit entsprechenden Rechten genehmigt werden.

Erstellen von Vorlagen

Sie können eine Vorlage von Richtlinieneinstellungen erstellen, die bei der Erstellung oder Aktualisierung von Gruppenrichtlinienobjekten verwendet werden soll.

Gehen Sie folgendermaßen vor, um eine Vorlage zu erstellen:

1. Erweitern Sie den Versionsüberprüfungs-Stammcontainer oder Untercontainer, klicken Sie mit der rechten Maustaste und wählen Sie dann **Neu | Vorlage**.
2. Geben Sie einen Namen und bei Bedarf eine Beschreibung für die Vorlage ein.

   Sie können jetzt Richtlinien auswählen, die in die Vorlage aufgenommen werden sollen.
3. Klicken Sie auf die Registerkarte **Details** und klicken Sie dann auf **Hinzufügen**.
4. Wählen Sie die gewünschten Richtlinien aus und klicken Sie auf **Hinzufügen**.
5. Wählen Sie die Vorlage aus und klicken Sie auf **Ändern**, um die Richtlinieneinstellungen zu konfigurieren.
6. Geben Sie die geforderten Informationen ein und klicken Sie auf **OK**.
7. Klicken Sie auf **OK**, wenn Sie alle erforderlichen Richtlinieneinstellungen hinzugefügt haben.

Die Vorlage muss den Genehmigungs- und Bereitstellungsprozess durchlaufen, bevor Sie angewandt werden kann.

Erstellen von Vorlagen ausgehend von registrierten Gruppenrichtlinienobjekten

Um die Übertragbarkeit von Vorlagen zu nutzen, können Sie vorhandene Gruppenrichtlinienobjekte und deren Einstellungen in Vorlagen konvertieren.

Alle in Quest Group Policy Manager-Vorlagen verwendeten ADM-Dateien müssen dem Unicode-Format entsprechen.

Gehen Sie folgendermaßen vor, um eine Vorlage von einem Gruppenrichtlinienobjekt zu erstellen:

1. Erweitern Sie den „Versionsüberprüfungs-Root" oder einen Untercontainer.
2. Klicken Sie mit der rechten Maustaste auf das entsprechende Gruppenrichtlinienobjekt und wählen Sie **Vorlagen | Vorlage erstellen**.
3. Wählen Sie den Container aus, in dem Sie die Vorlage speichern möchten, und klicken Sie auf **OK**.

   – ODER –

   Klicken Sie auf **Neuen Ordner erstellen**, um einen neuen Container zu erstellen, geben Sie einen Namen für den Container ein und klicken Sie dann auf **OK**.

   Sie können diese Vorlage jetzt auf andere Gruppenrichtlinienobjekte anwenden.

Arbeiten mit registrierten Objekten

Unabhängig vom Status des registrierten Gruppenrichtlinienobjekts, der WMI-Filter, der Vorlagen, der Domäne, der Site oder der Organisationseinheit (Verfügbar, Ausgebucht, Anstehende Genehmigung und Anstehende Bereitstellung) können Sie die folgenden Aufgaben durchführen, wenn Ihnen die entsprechende Rolle zugewiesen ist:

- Erstellen von Bezeichnungen
- Anzeigen des Verlaufs
- Anzeigen und Bearbeiten von Eigenschaften
- Anzeigen der Versionsunterschiede
- Erstellen eines Berichts
- Arbeiten mit verfügbaren Objekten
- Importieren von Objekten

Erstellen von Bezeichnungen

Sie können benutzerdefinierte Verlaufskommentare (Bezeichnungen) zu Objekten und Containern im Versionsüberprüfungssystem hinzufügen. Diese Funktion ermöglicht es den Benutzern, einen Rollback zu einem durch eine bestimmte Bezeichnung gekennzeichneten Objekt durchzuführen.

Gehen Sie folgendermaßen vor, um eine Bezeichnung zu erstellen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie das erforderliche Objekt aus.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Bezeichnung**.
3. Geben Sie die Bezeichnung in das Dialogfeld „Kommentar" ein und klicken Sie dann auf **OK**.

Anzeigen des Verlaufs

Sie können auf einfache Weise einen Bericht erstellen, der die historischen Einstellungen für Objekte im Versionsüberprüfungssystem oder einen Vergleich der Versionen anzeigt.

Gehen Sie folgendermaßen vor, um den Verlauf anzuzeigen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf ein Objekt und wählen Sie **Verlauf anzeigen**.
3. Wählen Sie eine Version aus der Liste aus.
4. Wählen Sie, falls vorhanden, erweiterte Optionen und Filteroptionen aus, die Sie aufnehmen möchten, klicken Sie mit der rechten Maustaste und wählen Sie dann **Ansicht**, um die historischen Informationen anzuzeigen.
5. Um den Unterschied zwischen verschiedenen Einbuchungen anzuzeigen, wählen Sie die erforderlichen Versionen aus und klicken Sie auf **Unterschiede**.
6. Klicken Sie auf **Drucken**, um den Bericht zu drucken.

   – ODER –

   Klicken Sie auf **Speichern unter**, um den Bericht im HTML-Format zu speichern.
7. Klicken Sie auf **Schließen**.

Anzeigen und Bearbeiten von Eigenschaften

Sie können auf einfache Art und Weise die Details für die aktuelle Version eines Objekts im Versionsüberprüfungssystem einschließlich der Sicherheit, der Benachrichtigungseinstellungen und der Genehmigungen anzeigen und bearbeiten.

Benutzer mit der entsprechenden Berechtigung können die Sicherheitseinstellungen ändern. Weitere Informationen finden Sie unter „Konfigurieren der rollenbasierten Delegation“ auf Seite 28.

Gehen Sie folgendermaßen vor, um die Eigenschaften anzuzeigen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root“ und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf das entsprechende Objekt und wählen Sie **Eigenschaften**.
3. Klicken Sie im Dialogfeld „Eigenschaften“ auf die entsprechende Registerkarte, um die zugehörigen Informationen anzuzeigen.

OPTION	BESCHREIBUNG
Allgemeines	Zeigen Sie die Domäne, den Benutzer, das Erstellungs- und Änderungsdatum, die Version, die eindeutige ID und den Gruppenrichtlinienobjektstatus an.
Verknüpfungen (ausgehend von der Seite „Gruppenrichtlinienobjekteigenschaften“)	Bearbeiten Sie die Verknüpfung zum Verwaltungsbereich.
Sicherheit	Delegieren Sie die Verantwortung über den Container.
Benachrichtigung	Wählen Sie aus, über welche Ereignisse eine Benachrichtigung erfolgen soll.
Genehmigungen	Anzahl der erforderlichen Genehmiger, Liste derjenigen, die ihre Genehmigung bereits erteilt haben, und Datum/Uhrzeit aller geplanten Bereitstellungen.

Anzeigen der Versionsunterschiede

Sie können einen Bericht erstellen, der die Unterschiede zwischen den Einstellungen von zwei beliebigen Objekten anzeigt.

Gehen Sie folgendermaßen vor, um die Unterschiede zwischen Einstellungen anzuzeigen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf zwei ähnliche Objekte und wählen Sie **Berichte | Unterschiede**.
3. Wählen Sie die Objekte, die Sie vergleichen möchten, aus der Liste aus und klicken Sie dann auf **OK**.
4. Klicken Sie auf **Drucken**, um den Bericht zu drucken.

   – ODER –

   Klicken Sie auf **Speichern unter**, um den Bericht im HTML-Format zu speichern.
5. Klicken Sie auf **Schließen**.

Erstellen eines Berichts

Sie können Berichte erstellen, die die Details der kontrollierten Objekte sowie Diagnose- und Fehlerbehebungsinformationen anzeigen. Weitere Informationen finden Sie unter „Berichte erstellen" auf Seite 85.

Arbeiten mit verfügbaren Objekten

Mit verfügbaren Objekten können Sie all die Aufgaben von registrierten Objekten (Verlauf anzeigen, Berichte über aktive Objekte anzeigen, Eigenschaften anzeigen, Objekt aus der Registrierung entfernen, Bezeichnungen erstellen und Objekte importieren/exportieren) und darüber hinaus die folgenden Aktionen durchführen:

- Ausbuchen von Objekten
- Einbuchen kontrollierter Objekte (Weitere Informationen finden Sie unter „Bearbeiten von Objekten“ auf Seite 74)
- Anfordern der Löschung eines Objekts
- Anfordern der Genehmigung
- Überprüfen der Konformität (Weitere Informationen finden Sie unter „Überprüfen der Konformität“ auf Seite 71)

Ausbuchen von Objekten

Bevor Benutzer registrierte Objekte bearbeiten können, müssen diese ausgebucht werden. Nachfolgend ist der Arbeitsablauf beschrieben: Buchen Sie das Objekt aus dem System aus, führen Sie die erforderlichen Bearbeitungsschritte durch und buchen Sie das geänderte Objekt wieder in das System ein.

Beim erstmaligen Ausbuchen eines Objekts wird eine Kopie des aktiven Originalobjekts erstellt.

Die Änderungen werden nur auf das aktive Unternehmen angewandt, wenn sie von den Benutzern mit der Berechtigung zum Genehmigen/Zurückweisen genehmigt und von Benutzern mit der Berechtigung zum Bereitstellen bereitgestellt wurden.

Die Versionsinformationen werden im Verlauf des Systems aktualisiert, wenn das Objekt wieder eingebucht wird. Es kann nur jeweils eine Person innerhalb des Systems ein Objekt ausbuchen und damit arbeiten.

Wenn Sie über alle erforderlichen Rechte verfügen, können Sie auch ein Objekt im ausgebuchten Status bereitstellen. In diesem Fall werden alle Schritte des Arbeitsablaufs automatisch durchgeführt.

Gehen Sie folgendermaßen vor, um ein Objekt auszubuchen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf ein Objekt mit dem Status „Verfügbar" und wählen Sie dann **Ausbuchen**.

Wenn ein Gruppenrichtlinienobjekt ausgebucht ist, werden nur die Einstellungen beibehalten – nicht die Gruppenrichtlinienobjekt-verknüpfungen. Sie können mehrere Gruppenrichtlinienobjekte gleichzeitig ausbuchen.

3. Geben Sie einen Kommentar ein und klicken Sie auf **OK**.

Anfordern der Löschung eines Objekts

Benutzer können das Löschen von Objekten in der Unternehmensumgebung, die aktuell im Versionsüberprüfungssystem registriert und sich im Status „Verfügbar" befinden, vorschlagen. Wenn die Anforderung genehmigt wird, wird das Objekt aus dem System entfernt und dann aus der aktiven Unternehmensumgebung gelöscht.

Gehen Sie folgendermaßen vor, um ein Objekt zu löschen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf das entsprechende Objekt und wählen Sie **Löschen**.
3. Geben Sie einen Kommentar ein und klicken Sie auf **OK**.

   Das Objekt befindet sich jetzt im Status „Anstehende Genehmigung". Eine Benachrichtigung bezüglich der Anforderung zum Löschen wird an die Benutzer mit der Berechtigung zum Genehmigen/ Zurückweisen gesendet.

Objekte mit der Versionsnummer 0.0 können von dem Benutzer gelöscht werden, der sie erstellt hat.

Anfordern der Genehmigung

Wenn ein Objekt geändert und in das System eingebucht wurde, können Sie die Benutzer mit der Berechtigung zum Genehmigen/Zurückweisen darüber benachrichtigen, dass die Aktualisierung bereit für das Genehmigungsverfahren ist.

Sie können auch die Genehmiger zum Zeitpunkt der Einbuchung benachrichtigen, wenn Sie wissen, dass Sie das Objekt nicht weiter verändern möchten. Weitere Informationen finden Sie unter „Einbuchen kontrollierter Objekte" auf Seite 63.

Gehen Sie folgendermaßen vor, um eine Genehmigung anzufordern:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf das geänderte Objekt und wählen Sie dann **Genehmigung anfordern**.
3. Geben Sie einen Kommentar ein und klicken Sie auf **OK**.

   Das Objekt befindet sich jetzt im Status „Anstehende Genehmigung".

Arbeiten mit ausgebuchten Objekten

Mit ausgebuchten Objekten können Sie all die Aufgaben von registrierten Objekten (Verlauf anzeigen, Berichte über aktive Objekte anzeigen, Eigenschaften anzeigen, Objekt aus der Registrierung entfernen, Bezeichnungen erstellen und Objekte importieren/exportieren) und darüber hinaus die folgenden Aktionen durchführen:

- Rückgängig machen einer Ausbuchung
- Einbuchen kontrollierter Objekte (Weitere Informationen finden Sie unter „Bearbeiten von Objekten“ auf Seite 74)
- Einbuchen kontrollierter Objekte
- Wiederherstellen einer vorigen Version
- Überprüfen der Konformität (Weitere Informationen finden Sie unter „Überprüfen der Konformität“ auf Seite 71)

Wenn Sie über alle erforderlichen Rechte verfügen, können Sie auch ein Objekt im ausgebuchten Status bereitstellen. In diesem Fall werden alle Schritte des Arbeitsablaufs automatisch durchgeführt.

Rückgängig machen einer Ausbuchung

Der Benutzer, der ein Objekt ausgebucht hat, hat die Möglichkeit, die Ausbuchung rückgängig zu machen und den Status des Objekts wieder in „Verfügbar“ zu ändern.

Gehen Sie folgendermaßen vor, um eine Ausbuchung rückgängig zu machen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root“ und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie dann **Ausbuchung rückgängig machen**.
3. Geben Sie einen Kommentar ein und klicken Sie auf **OK**.

Wenn Sie das Ausbuchen eines Objekts der Version 0.0 rückgängig machen, wird die Arbeitskopie gelöscht und es gibt keine Eintragung des Objekts im Versionsüberprüfungssystem.

Einbuchen kontrollierter Objekte

Wenn Sie ein Objekt ausgebucht und dessen Einstellungen bearbeitet haben, stehen folgende Optionen zur Auswahl:

- Einbuchen von Objekten in ihrem aktuellen Status für weitere Aktualisierungen
- Einbuchen von Objekten und Benachrichtigen der Genehmiger, dass das Objekt bereit für die Genehmigung oder Zurückweisung ist
- Rückgängigmachung der Ausbuchung (Weitere Informationen finden Sie unter „Rückgängig machen einer Ausbuchung“ auf Seite 62)

Eine Einbuchung aktualisiert den Verlauf des Objekts innerhalb des Versionsüberprüfungssystems mit den Änderungen, die vorgenommen wurden, während es ausgebucht war. Jede Einbuchung ist mit einem Kommentar und einer eindeutigen Versionsnummer hinter dem Dezimalpunkt (wie etwa v1.1) verbunden.

Eine Einbuchung ermöglicht nicht die Implementierung der Offline-Änderungen in die aktive Unternehmensumgebung, da die Änderungen zunächst von einem Genehmiger genehmigt werden müssen. Wenn sich ein Objekt im Status „Anstehende Genehmigung“ befindet, kann es nicht von einem anderen Benutzer des Systems ausgebucht werden.

Es können mehrere Einbuchungen und Ausbuchungen im System durchgeführt werden, ohne dass hierzu eine Genehmigung erforderlich wäre. Wenn ein Benutzer ein Objekt einbucht, so dass es für einen anderen Benutzer des Systems verfügbar ist, arbeitet der nächste Benutzer, der dasselbe Objekt ausbucht, mit der aktuellen Offline-Version einschließlich aller bis dahin getätigten Änderungen. Nachdem alle Benutzer ihre erforderlichen Änderungen am Offline-Objekt vorgenommen haben, wird es vom Genehmigungssystem verarbeitet, um zu ermitteln, ob die Änderungen aktiv im Unternehmen übernommen werden dürfen oder nicht.

Gehen Sie folgendermaßen vor, um ein Objekt einzubuchen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf ein Objekt und wählen Sie **Einbuchen**.
3. Geben Sie bei Bedarf einen Kommentar ein.
4. Klicken Sie auf **OK**.
5. Wählen Sie **Genehmigung anfordern**, falls erforderlich.
6. Klicken Sie auf **OK**.

Zurückziehen der Genehmigungsanforderung

Jeder Benutzer, der eine Änderung an einem Objekt vorschlägt, kann seine eigene Genehmigungsanforderung zurückziehen, wenn sich die Änderung noch im Status „Anstehende Genehmigung" befindet und noch keine Genehmigungen erteilt worden sind.

Gehen Sie folgendermaßen vor, um eine Genehmigungsanforderung zurückzuziehen:

1. Klicken Sie mit der rechten Maustaste auf ein Objekt mit dem Status „Anstehende Genehmigung" und wählen Sie **Genehmigungs-anforderung zurückziehen**.
2. Klicken Sie auf **OK**.

   Das Objekt wird in den Status „Verfügbar" zurückversetzt.

Genehmigungsanforderungen können nicht für geplante Genehmigungen zurückgezogen werden. Sie können auch nicht zurückgezogen werden, wenn bereits eine Genehmigung einer Bearbeitung, die mehrere Genehmigungen erfordert, erteilt worden ist.

Wiederherstellen einer vorigen Version

Sie können auf einfache Weise einen Bericht erstellen, der die historischen Einstellungen für Objekte im Versionsüberprüfungssystem oder einen Vergleich der Versionen zur Ermittlung von Unterschieden anzeigt. Weitere Informationen finden Sie unter „Erstellen von Bezeichnungen“ auf Seite 55.

Sie können auch Einstellungen von jeder Version eines Objekts im Verlauf des Versionsüberprüfungssystems importieren. Dieser Vorgang wirkt sich nur auf das System und nicht auf die aktive Unternehmensumgebung aus, bis der gesamte Genehmigungsprozess abgeschlossen ist. Sie müssen das Objekt ausgebucht haben, um diesen Vorgang durchführen zu können. Nachdem Sie sich entschlossen haben, einen Rollback für eine bestimmte Version durchzuführen, werden die Einstellungen der aktuell ausgebuchten Version mit den Einstellungen der aus dem Verlauf ausgewählten, gewünschten Version überschrieben.

Von diesem Punkt an wird der grundlegende Arbeitsablauf des Systems wieder fortgesetzt, und Sie müssen die Änderungen einbuchen und genehmigen, um sie in die aktive Unternehmensumgebung zu übernehmen.

Gehen Sie folgendermaßen vor, um den Verlauf anzuzeigen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root“ und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf ein Objekt und wählen Sie **Verlauf anzeigen**.

   Das Datum, das Konto, die Version, der Kommentar und der entsprechende Vorgang, der zur Erzeugung des Verlaufselements geführt hat, werden angezeigt.
3. Wählen Sie ggf. die erweiterten Optionen und die Filteroptionen, die Sie aufnehmen möchten.
4. Um die Einstellungen einer früheren Version anzuzeigen, wählen Sie die Version aus und klicken dann auf **Ansicht**.
5. Um die Unterschiede zwischen den Einstellungen verschiedener Versionen anzuzeigen, wählen Sie die entsprechenden Versionen aus und klicken dann auf **Unterschiede**.
6. Um die Einstellungen einer früheren Version zu importieren, wählen Sie die entsprechende Version aus und klicken dann auf **Download von**.
7. Wählen Sie, welche Einstellungen und Optionen Sie überschreiben möchte, und klicken Sie dann auf **OK**.
8. Klicken Sie auf **Schließen**.

Arbeiten mit zur Genehmigung und Bereitstellung anstehenden Objekten

Nur Benutzer mit der Berechtigung zum Genehmigen/Zurückweisen können jegliche anstehende Genehmigungsanforderungen von den normalen Systembenutzern genehmigen oder zurückweisen. Nur Benutzer mit der Berechtigung zum Bereitstellen können die Änderungen auf die aktive Unternehmensumgebung anwenden. Das Genehmigungssystem schützt die aktive Unternehmensumgebung vor jeglichen unbefugten Änderungen am aktiven System, die zu ungewünschten Ergebnissen führen könnten.

Die folgenden Anforderungen von den Benutzern erfordern eine Genehmigung:

- Änderungen an Offline-Objekten, die in die aktive Umgebung übernommen werden sollen
- Erstellung neuer Objekte
- Löschen vorhandener Objekte

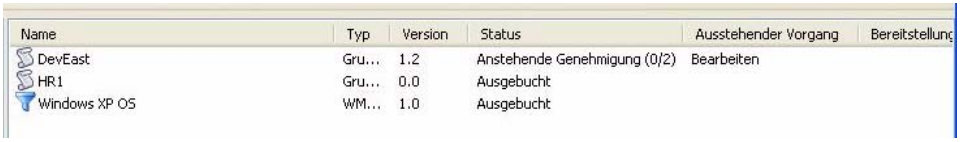
Mit Hilfe des Exportassistenten können Sie Gruppenrichtlinienobjekte offline testen, bevor diese in das aktive Unternehmen implementiert werden. Weitere Informationen finden Sie unter „Arbeiten mit verfügbaren Objekten“ auf Seite 59.

Weitere Informationen finden Sie unter „Konfigurieren von Genehmigern auf mehreren Ebenen“ auf Seite 67, „Genehmigen und Zurückweisen von Bearbeitungen“ auf Seite 68 und „Planen der Bereitstellung“ auf Seite 69.

Konfigurieren von Genehmigern auf mehreren Ebenen

Sie haben die Möglichkeit, einen weiteren Schutz zu implementieren, indem Sie Genehmiger auf mehreren Ebenen benennen. Bei Auswahl dieser Option muss eine Änderung von der angegebenen Anzahl von Genehmigern genehmigt werden, bevor sie für die Bereitstellung in der aktiven Umgebung verfügbar ist.

Die Listenansicht zeigt die Anzahl der erforderlichen Genehmigungen sowie die Anzahl der bislang erfolgten Genehmigungen. Im Beispiel unten erfordert eine Bearbeitung nur eine einzige Genehmigung; dagegen erfordert eine Erstellung die Genehmigung auf einer zweiten Ebene.



Die Genehmigung auf mehreren Ebenen wird innerhalb der Servereigenschaften konfiguriert. Weitere Informationen über die Konfiguration dieser Option finden Sie unter „Konfigurieren des Versionsüberprüfungsservers“ auf Seite 22.

Bevor die endgültige Genehmigung erteilt wird und die Änderungen bereitgestellt wurden,

- hat jeder Genehmiger das Recht, seine Genehmigung zurückzuziehen (klicken Sie hierzu einfach mit der rechten Maustaste auf das zur Genehmigung anstehende Objekt und wählen Sie Genehmigung zurückziehen);
- kann jeder anstehende Vorgang zurückgewiesen werden.

Genehmigen und Zurückweisen von Bearbeitungen

Wenn ein Objekt eingebucht wurde und der Genehmiger benachrichtigt wurde, dass die Offline-Änderungen zur Genehmigung bereit sind, werden die Änderungen entweder genehmigt oder zurückgewiesen.

Bevor die Genehmigung einer Änderung in Kraft tritt, erkennt das Versionsüberprüfungssystem, ob ein Objekt unbekannterweise oder außerhalb des Verwaltungsbereichs des Systems (etwa durch systemeigene Tools) geändert wurde, und fordert den Genehmiger auf, die entsprechende Maßnahme zu ergreifen. Der Genehmiger kann das Objekt überschreiben oder in seinem aktuellen Zustand belassen.

WENN DIE ÄNDERUNGEN GENEHMIGT UND BEREITGESTELLT WURDEN	WENN DIE ÄNDERUNGEN ZURÜCKGEWIESEN WURDEN
• Die Einstellungen werden auf das aktive Objekt angewandt, und die Stelle vor dem Dezimalpunkt der Versionsnummer wird inkrementiert (Beispiel: v2.0). • Die Einstellungen des Offline-Objekts werden auf das aktive Objekt angewandt. Beim nächsten Ausbuchen wiederholt der Prozess die Erstellung einer neuen Offline-Kopie des aktiven Gruppenrichtlinienobjekts. Hinweis: Wenn die Änderungen nur genehmigt, jedoch nicht bereitgestellt sind, wird der Status in „Anstehende Bereitstellung" geändert, und die entsprechenden Gruppenrichtlinien-objekte werden im Suchordner „Anste-hende Bereitstellung" angezeigt.	• Es passiert nichts, und der Status wird auf „Verfügbar" zurückgesetzt, so dass das Objekt wieder ausgebucht werden kann.

Sie folgendermaßen vor, um Bearbeitungen am Gruppenrichtlinienobjekt zu genehmigen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf ein kontrolliertes Objekt mit dem Status „Anstehende Genehmigung" und wählen Sie **Genehmigen**.

   Wenn Sie über die erforderliche Berechtigung verfügen, können Sie auch zu diesem Zeitpunkt die Option zum Bereitstellen der Aktualisierungen für das Unternehmen auswählen. Falls nicht, wird das Objekt in den Status „Anstehende Bereitstellung" versetzt.

Gehen Sie folgendermaßen vor, um Bearbeitungen zurückzuweisen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf ein kontrolliertes Objekt mit dem Status „Anstehende Genehmigung" und wählen Sie **Ablehnen**.
3. Geben Sie einen Kommentar ein und klicken Sie auf **OK**.

Planen der Bereitstellung

Die Bereitstellung von Änderungen innerhalb des Systems ist ein kritischer Prozess, der Auswirkungen auf die aktive Umgebung hat. Um die Auswirkungen der Unterbrechung zu minimieren, sollte dieses Verfahren während eines Zeitraums ausgeführt werden, in dem die Auswirkungen auf die Benutzer minimal sind, da die Änderungen das Verhalten bestimmter Systeme verändern können.

Um das Auftreten möglicher Probleme zu verringern, können Sie die Bereitstellung der Änderungen zu einem bestimmten Datum und zu einer bestimmten Uhrzeit planen, das bzw. die Ihren Bedürfnissen am besten entspricht.

Wenn Sie über mehrere Genehmiger verfügen

- ist die Planungsfunktion nur während der endgültigen Genehmigung und der Bereitstellung verfügbar;
- wird, wenn die geplante Genehmigung aufgrund einer Nichtkonformität oder aus irgendeinem anderen Grund fehlschlägt, der Bereitsteller benachrichtigt;
- kann nur der Bereitsteller die geplante Bereitstellung abbrechen.

Gehen Sie folgendermaßen vor, um Bearbeitungen zu genehmigen und bereitzustellen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf ein Objekt mit dem Status „Anstehende Genehmigung" und wählen Sie **Genehmigen**.

   Sie können jetzt das Objekt in der Umgebung bereitstellen, wenn Sie der endgültige Genehmiger sind und über die Berechtigung zum Bereitstellen verfügen.

   Sie können die Änderungen sofort oder zu einem bestimmten Zeitpunkt bereitstellen.

   Wenn Sie „Bereitstellung an einem späteren Datum planen" auswählen, dann wählen Sie ein Datum aus der Liste, wählen Sie dann den Zeitbereich, den Sie anpassen möchten, und geben Sie manuell die gewünschte Uhrzeit sowie einen Kommentar ein. Klicken Sie anschließend auf OK.

   Wenn Sie eine Uhrzeit festgelegt haben, wird ein Uhr-Symbol neben dem Objekt angezeigt. Außerdem werden das Datum und die Uhrzeit in der Spalte „Genehmigungen" angezeigt.

Wenn eine geplante Genehmigung aus irgendeinem Grund fehlschlägt, wird die Bereitstellung des Objekts abgebrochen, und das Objekt bleibt im Status „Anstehende Bereitstellung".

Gehen Sie folgendermaßen vor, um eine Bereitstellung erneut zu planen:

1. Klicken Sie mit der rechten Maustaste auf das kontrollierte Objekt und wählen Sie **Bereitstellen**.
2. Wählen Sie ein neues Datum aus der Liste, wählen Sie dann den Zeitbereich, den Sie anpassen möchten, und geben Sie manuell die gewünschte Uhrzeit sowie einen Kommentar ein. Klicken Sie anschließend auf **OK**.

Überprüfen der Konformität

Group Policy Manager ermöglicht Ihnen zu ermitteln, ob ein Objekt außerhalb des Bereichs des Systems in der aktiven Unternehmensumgebung geändert wurde. Wenn eine Diskrepanz zwischen der letzten zurückliegenden Sicherung und dem aktiven Objekt festgestellt wird, dann ist ein Benutzer mit den entsprechenden Berechtigungen in der Lage, folgende Vorgänge durchzuführen:

- Rollback: Wiederherstellen des letzten im System gespeicherten Status des Objekts in der aktiven Umgebung durch Überschreiben der letzten unzulässigen Änderung.
- Integrieren in aktive Umgebung: Akzeptieren, dass die Änderungen am Gruppenrichtlinienobjekt zulässig sind und das Objekt aktueller als die im System vorhandene Version ist. Dies führt zur automatischen Sicherung dieser Änderungen im System und zur Inkrementierung der Stelle vor dem Dezimalpunkt der Versionsnummer der Sicherung.
- Belassen des aktiven Objekts in seinem nicht konformen Status.

Wenn ein Objekt in der aktiven Umgebung gelöscht wurde, ist ein Benutzer mit den entsprechenden Berechtigungen in der Lage, folgende Aktionen auszuführen:

- Wiederherstellen des Objekts in der aktiven Umgebung
- Entfernen des Objekts aus der Registrierung des Versions-überprüfungssystems

Wenn ein SOM gelöscht wurde, haben Sie nur die Möglichkeit, das Objekt aus der Registrierung zu entfernen.

Gehen Sie folgendermaßen vor, um zu gewährleisten, dass alle registrierten Objekte sich seit ihrer letzten Sicherung nicht geändert haben:

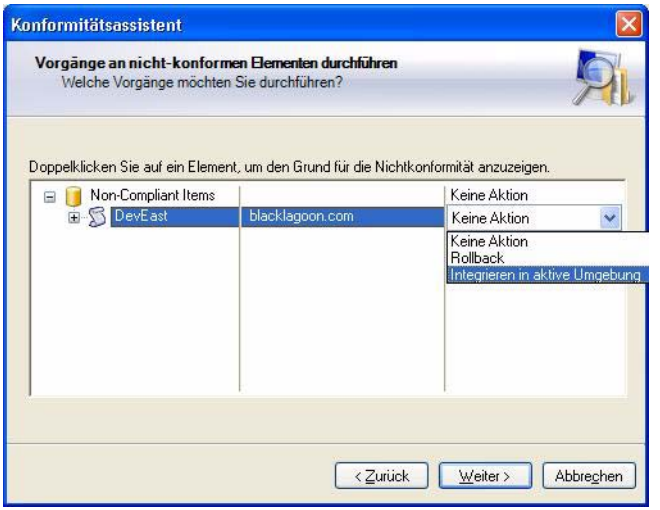
1. Klicken Sie mit der rechten Maustaste auf den Versionsüberprüfung-Stammknoten oder Untercontainer und wählen Sie dann **Konformität prüfen**.

   – ODER –

   Wählen Sie das erforderliche Objekt aus, klicken Sie mit der rechten Maustaste und wählen Sie dann **Erweitert | Konformität prüfen**.

2. Klicken Sie auf **Weiter**, um die Konformitätsprüfung auszuführen.
   Die nicht konformen Objekte werden angezeigt.

3. Wählen Sie die erforderlichen Aktionen, indem Sie auf das Feld „Aktion" klicken, um die Liste der Optionen anzuzeigen, und klicken Sie dann auf **Weiter**.



4. Klicken Sie auf **Fertig stellen**.

Verwenden der Befehlszeilenschnittstelle zur Überprüfung der Konformität

Der Konformitätsassistent verfügt außerdem über eine Befehlszeilenschnittstelle, um Sie bei der Automatisierung all seiner Aufgaben zu unterstützen (Rollback zur vorigen Version, Integrieren von Bearbeitungen, Überprüfen der Konformität, Unterdrückung der Aufforderung zur Bestätigung).

```
C:\Programme\Quest Software\Quest Group Policy Manager>compliance ?

Compliance Command Line Utility - Version 4.1.0.0.
Copyright Quest Software 2004-2007. Alle Rechte vorbehalten.

Alle Umschaltungen müssen mit '/' oder '-' beginnen.

Die Syntax des Befehls lautet:

Compliance.exe [/s server] [/u username] [/p password]

       [/d domainToCheck] [/o objectVcIdToCheck]

       [/a (RollBack|Incorporate)]

/s  Der Server und Port des QGPM-Diensts im Format 'Server:Port'.

     Falls nicht anders angegeben lautet die Standardeinstellung
     'localhost:40200'

/u   Geben Sie bei Angabe anderer Anmeldeinformationen als die des
     angemeldeten Benutzers den Benutzernamen im Format Domäne\
     Konto an.

/p   Geben Sie bei Angabe anderer Anmeldeinformationen als die des
     angemeldeten Benutzers hier das Kennwort an.

/d   Geben Sie eine kontrollierte Domäne für die Überprüfung der
     Konformität an. Alle Objekte in der Domäne werden überprüft.
     Diese Option kann mehr als einmal verwendet werden.

/o   Geben Sie die Versionsüberprüfungs-ID eines Objekts auf dem
     angegebenen Server an, dessen Konformität überprüft wird. Diese
     Option kann mehr als einmal verwendet werden.

/a   Geben Sie einen Vorgang an, der bei Feststellung eines nicht-
     konformen Objekts ausgeführt werden soll.
```

```
Die zulässigen Parameter sind entweder 'RollBack', um das aktive
Objekt auf seine letzte bekannte gültige Sicherung zurückzusetzen,
oder 'Incorporate', um das geänderte aktive Objekt in das
Versionsüberprüfungssystem zu überführen. Falls nicht angegeben
werden keine Änderungen durchgeführt.

Wenn weder /d noch /o verwendet wird, dann werden alle Elemente auf
dem Server aufgelistet und auf Ihre Konformität hin überprüft.
```

Bearbeiten von Objekten

- Gruppenrichtlinienobjekt bearbeiten
- Anwenden von Vorlagen
- Bearbeiten von WMI-Filtern
- Verknüpfen von Gruppenrichtlinienobjekten
- Bearbeiten von Vorlagen
- Importieren der INF-Dateieinstellungen

Gruppenrichtlinienobjekt bearbeiten

Wenn Sie ein Gruppenrichtlinienobjekt ausgebucht haben, können Sie seine Einstellungen im Gruppenrichtlinien-Editor bearbeiten, Sicherheits- und WMI-Filter erstellen und die Computer- und Benutzereinstellungen aktivieren/ deaktivieren.

Da Sie Gruppenrichtlinienobjekte nur mit Sites, Domänen und Organisationseinheiten verknüpfen können, unterstützt Sie die Konfiguration von Sicherheitsfiltern bei der Verfeinerung der Übernahme von Gruppenrichtlinienobjekteinstellungen für eine Gruppe, für einen Benutzer oder für einen Computer.

Die Benutzer und Computer, die Sie beim Einstellen der Sicherheitsfilterung auswählen, müssen über die Berechtigung sowohl zum Lesen als auch zur Übernahme von Gruppenrichtlinien für das entsprechende Gruppenrichtlinienobjekt verfügen.

Wenn Sie ein Gruppenrichtlinienobjekt ausbuchen, werden die Änderungen an einer Kopie des aktiven Gruppenrichtlinienobjekts vorgenommen. Die Änderungen, die Sie vornehmen, haben keinen Einfluss auf die Gruppenrichtlinienobjekteinstellungen im Unternehmen, bis diese genehmigt und bereitgestellt werden.

Sie können auch Gruppenrichtlinienobjekte durch Übernehmen von Vorlagen bearbeiten. Gruppenrichtlinienobjekte müssen ausgebucht werden, bevor Sie eine Vorlage auf diese Objekte anwenden können. Wenn Sie eine Vorlage auf ein Gruppenrichtlinienobjekt anwenden, wenden Sie die im Versionsüberprüfungssystem gespeicherte Hauptversion an. Weitere Informationen finden Sie unter „Ausbuchen von Objekten“ auf Seite 60 und „Anwenden von Vorlagen“ auf Seite 77.

Gehen Sie folgendermaßen vor, um Gruppenrichtlinienobjekteinstellungen zu bearbeiten:

1. Klicken Sie mit der rechten Maustaste auf ein ausgebuchtes Gruppenrichtlinienobjekt und wählen Sie **Bearbeiten**.
2. Klicken Sie auf **Editor starten**, nehmen Sie die erforderlichen Änderungen vor und schließen Sie den Gruppenrichtlinien-Editor.

   Wenn Sie Gruppenrichtlinienobjekte registrieren, bleibt der Gruppenrichtlinienobjektstatus (Computer- und Benutzereinstellungen aktiviert/deaktiviert) erhalten. Bei Bedarf können Sie diese Einstellungen jedoch auch leicht ausgehend vom Versionsüberprüfungssystem ändern.
3. Aktivieren bzw. deaktivieren Sie die Benutzer- und Computereinstellungsoptionen wie erforderlich.
4. Wählen Sie erforderlichenfalls die Registerkarte „Sicherheit“ und klicken Sie dann auf **Hinzufügen**, geben Sie den erforderlichen Benutzer, Computer, oder die erforderliche Gruppe ein oder suchen Sie danach und klicken Sie dann auf **OK**.

   – ODER –

   Um die aktuellen Sicherheitsfilter zu ändern, wählen Sie den entsprechenden Eintrag aus und klicken dann auf **Entfernen**.
5. Klicken Sie auf die Schaltfläche **Erweitert**, um die erweiterten Berechtigungen auszuwählen.

6. Um das Gruppenrichtlinienobjekt mit einem bereits in der Domäne vorhandenen WMI-Filter zu verknüpfen, wählen Sie die Registerkarte WMI-Filter und anschließend den Filter aus dem Dropdown-Listenfeld aus.

   Bei Genehmigung wird die Verknüpfung zum Gruppenrichtlinienobjekt hinzugefügt.

   – ODER –

   Um eine vorhandene WMI-Filterung zu entfernen, wählen Sie **Keine**.

   Wenn das Gruppenrichtlinienobjekt zuvor mit einem WMI-Filter verknüpft war, dann wird die Verknüpfung des Gruppenrichtlinienobjekts mit dem Filter bei Genehmigung aufgehoben.

7. Klicken Sie auf **OK**.

   Sie haben jetzt die Möglichkeit, das Gruppenrichtlinienobjekt einzubuchen und für eine spätere Verwendung zu speichern oder einzubuchen und die Genehmigung der Änderungen anzufordern.

Anwenden von Vorlagen

Vorlagen können nur auf registrierte Gruppenrichtlinienobjekte innerhalb des Versionsüberprüfungssystems angewandt werden. Wenn Sie eine Vorlage anwenden, werden Änderungen an den Gruppenrichtlinienobjekteinstellungen vorgenommen; daher müssen sie denselben Genehmigungsprozess durchlaufen wie alle anderen an den Gruppenrichtlinienobjekten im System vorgenommenen Änderungen. Nachfolgend ist der Arbeitsablauf beschrieben:

- Ausbuchen des Gruppenrichtlinienobjekts
- Anwenden einer Vorlage
- Einbuchen der Änderungen in das System

Überprüfen auf in Konflikt stehende Vorlageneinstellungen

Group Policy Manager führt eine Überprüfung auf in Konflikt stehende Vorlageneinstellungen durch, wenn Sie ein neues Gruppenrichtlinienobjekt erstellen und Vorlagen auf dieses Objekt anwenden oder wenn Sie ein Gruppenrichtlinienobjekt auswählen, das bereits erstellt wurde, und eine Vorlage auf dieses Objekt anwenden. Wenn zwei oder mehr Vorlagen ausgewählt sind, wird ein Dialogfeld geöffnet, und Sie haben die Möglichkeit, die Überprüfung auf Konflikte zu überspringen.

Wenn Konflikte festgestellt werden, können Sie den Vorgang fortsetzen, wobei die Einstellungen der letzten Vorlage Vorrang haben. Sie können die Details der in Konflikt stehenden Einstellungen anzeigen, indem Sie auf die Schaltfläche „Details" klicken. Hierdurch wird der Vorlagenkonfliktbericht angezeigt.

Gehen Sie folgendermaßen vor, um eine Vorlage anzuwenden:

1. Erweitern Sie den erforderlichen Container, Klicken Sie mit der rechten Maustaste auf das ausgebuchte Gruppenrichtlinienobjekt und wählen Sie dann **Vorlagen | Vorlagen übernehmen**.
2. Klicken Sie auf **Hinzufügen**, um eine oder mehrere Vorlagen auszuwählen.

   Wenn Sie mehr als eine Vorlage ausgewählt haben, können Sie die Schaltflächen „Nach oben" und „Nach unten" verwenden, um die Reihenfolge zu bestimmen, in der die Vorlagen angewandt werden. Die Reihenfolge der Anwendung ist von oben nach unten.
3. Klicken Sie auf **OK**.

Bearbeiten von WMI-Filtern

Gehen Sie folgendermaßen vor, um einen WMI-Filter zu bearbeiten:

1. Wählen Sie den WMI-Filter, den Sie bearbeiten möchten, in dem Versionsüberprüfungscontainer aus, in dem er gespeichert ist.
2. Klicken Sie mit der rechten Maustaste auf den WMI-Filter und wählen Sie **Bearbeiten**.
3. Bearbeiten Sie die Eigenschaften des WMI-Filters.
4. Klicken Sie auf **OK**.

   Sie haben jetzt die Möglichkeit, den WMI-Filter einzubuchen und für eine spätere Verwendung zu speichern oder einzubuchen und die Genehmigung der Änderungen anzufordern.

Verknüpfen von Gruppenrichtlinien-objekten

Wenn Gruppenrichtlinienobjekte erstellt und konfiguriert wurden, müssen Sie mit der entsprechenden Site, der entsprechenden Domäne oder der entsprechenden Organisationseinheit verknüpft werden. Bevor Sie ein Gruppenrichtlinienobjekt verknüpfen können, müssen Sie die Site, die Domäne oder die Organisations-einheit registrieren und ausbuchen. Weitere Informationen über das Registrieren eines Verwaltungsbereichs finden Sie unter „Registrieren von Objekten“ auf Seite 39.

Benutzer mit der Berechtigung zum Verknüpfen des Gruppenrichtlinienobjekts/ Aufheben der Verknüpfung des Gruppenrichtlinienobjekts können ein einzelnes Gruppenrichtlinienobjekt mit mehreren Sites, Domänen oder Organisations-einheiten und mehrere Gruppenrichtlinienobjekte mit einer Site, einer Domäne oder Organisationseinheit verknüpfen. Wenn Sie mehr als ein Gruppen-richtlinienobjekt verknüpfen, müssen Sie auf deren Reihenfolge achten. Das erste Gruppenrichtlinienobjekt hat die höchste Priorität, da es als letztes verarbeitet wird. Hieraus ergibt sich die Notwendigkeit eines Berichterstattungs-Tools, das alle Verknüpfungen und die aus der Vererbungsstruktur der Gruppen-richtlinien resultierende Richtlinienserie anzeigt.

Standardmäßig sind alle Benutzer und Computer, die an einer verknüpften Site, in einer verknüpften Domäne oder in einer verknüpften Organisationseinheit enthalten sind, von Gruppenrichtlinienobjekten betroffen.

Gehen Sie folgendermaßen vor, um ein Gruppenrichtlinienobjekt zu verknüpfen:

1. Klicken Sie mit der rechten Maustaste auf eine ausgebuchte Site, Domäne oder Organisationseinheit und wählen Sie dann **Bearbeiten**.
2. Klicken Sie auf **Neue Verknüpfung**, um eine weitere Zusammenstellung von Verwaltungsbereichen oder Gruppenrichtlinienobjekten hinzuzufügen.

Die Richtlinien werden gemäß der hierarchischen Struktur von Active Directory übernommen. Sie können mit den Pfeilschaltflächen die Reihenfolge ändern, in der die Gruppenrichtlinienobjekte angewandt werden.

3. Klicken Sie auf die Optionen **Aktiviert** und **Erzwungen**, wählen Sie die entsprechende Option aus, um die Gruppenrichtlinienobjektverknüpfung zu aktivieren bzw. zu erzwingen, und klicken Sie dann auf **OK**.
4. Aktivieren Sie erforderlichenfalls die Option **Vererbung deaktivieren**.
5. Klicken Sie auf **OK**.

   Wenn die Verknüpfung eines Gruppenrichtlinienobjekts nicht länger aktiviert oder erzwungen sein soll, deaktivieren Sie die Option und klicken Sie dann auf OK.

Bearbeiten von Vorlagen

Die an den Vorlageneinstellungen durchgeführten Änderungen müssen auf das Gruppenrichtlinienobjekt angewandt werden, um berücksichtigt zu werden. Weitere Informationen über das Anwenden von Vorlagen finden Sie unter „Anwenden von Vorlagen“ auf Seite 77.

Gehen Sie folgendermaßen vor, um eine Vorlage zu bearbeiten:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root“ und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf die entsprechende Vorlage und wählen Sie **Bearbeiten**.
3. Klicken Sie auf die Registerkarte **Details** und dann auf **Hinzufügen**.
4. Wählen Sie die gewünschten Richtlinien aus und klicken Sie auf **Hinzufügen oder Entfernen**.

   – ODER –

   Wählen Sie die Richtlinie, klicken Sie auf **Ändern**, um die Richtlinieneinstellungen zu konfigurieren, geben Sie die erforderlichen Informationen ein und klicken Sie dann auf **OK**.
5. Klicken Sie auf **OK**, wenn Sie alle erforderlichen Richtlinieneinstellungen hinzugefügt haben.

Importieren der INF-Dateieinstellungen

Sie können auf einfache Art und Weise Sicherheitsrichtlinieneinstellung aus einer INF-Datei in eine Vorlage importieren, dann die Vorlage bearbeiten und anschließend auf Gruppenrichtlinienobjekte anwenden.

Gehen Sie folgendermaßen vor, um INF-Datei zu importieren:

1. Erweitern Sie Quest Group Policy Manager und den Versionsüberprüfungs-Stammcontainer, klicken Sie mit der rechten Maustaste und wählen Sie dann **INF-Datei importieren**.
2. Wählen Sie die gewünschte Datei aus und klicken Sie auf **OK**.

Importieren und Exportieren

- Exportieren von Objekten
- Importieren von Objekten

Um in eine andere Domäne zu exportieren, muss GPMC auf dem Client installiert sein.

Exportieren von Objekten

Mit Hilfe des Exportassistenten können Sie Objekte offline testen, bevor diese in das aktive Unternehmen implementiert werden. Nachfolgend ist ein typisches Szenario aufgeführt:

- Buchen Sie ein Objekt aus und nehmen Sie die gewünschten Änderungen vor.

  Bevor Sie die Änderung einbuchen und eine Genehmigung anfordern, können Sie die vorgenommenen Änderungen testen.

- Exportieren Sie das Objekt in eine andere Domäne und testen Sie die Aktualisierungen.

  Bei Auftreten eines Problems können Sie dies in der Testdomäne beheben.

- Importieren des Objekts.
- Buchen Sie die neuen und verbesserten Änderungen zur Genehmigung ein.

Im Status „Anstehende Genehmigung" bietet der Export des Objekts eine zusätzliche Ebene der Qualitätskontrolle des Objekts, bevor die Änderungen in das aktive Unternehmen übernommen werden. Ein Mitglied der Genehmigergruppe kann das Objekt zur Überprüfung in eine Testumgebung exportieren, bevor es die Genehmigung erteilt oder die Änderungen zurückweist.

Gehen Sie folgendermaßen vor, um ein Objekt in eine Testumgebung zu exportieren:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf ein Objekt und wählen Sie **Exportieren**.
3. Wählen Sie die Version, die Sie testen möchten, und klicken Sie auf **Weiter**.
4. Wählen Sie das Ziel aus.

   Sie können ein lokales Verzeichnis oder eine Netzwerkfreigabe, ein anderes Versionsüberprüfungssystem oder eine Testdomäne im aktiven Netzwerk auswählen.

   Gehen Sie folgendermaßen vor, um ein lokales Verzeichnis oder eine Netzwerkfreigabe auszuwählen:

   a) Wählen Sie **Eine Sicherung auf der Festplatte** aus und klicken Sie dann auf **Weiter**.

   b) Wählen Sie das Sicherungsverzeichnis aus und klicken Sie dann auf **Weiter**.

   c) Klicken Sie auf **Fertig stellen**.

   Gehen Sie folgendermaßen vor, um eine Verbindung zum Versionsüberprüfungssystem herzustellen:

   a) Wählen Sie **Ein Versionsüberprüfungssystem** aus und klicken Sie dann auf **Weiter**.

   b) Wählen Sie die Zieldomäne aus und klicken Sie auf **Weiter**.

   c) Wählen Sie den Ordner aus, in dem Sie das exportierte Objekt speichern möchten, und klicken Sie dann auf **Weiter**.

   d) Wählen Sie (falls erforderlich) eine Migrationstabelle aus und klicken Sie dann auf **Weiter**.

   e) Klicken Sie auf **Fertig stellen**.

   f) Klicken Sie auf **Weiter**.

Gehen Sie folgendermaßen vor, um eine Testdomäne in der aktiven Umgebung auszuwählen:

a) Wählen Sie **Die aktive Umgebung** aus und klicken Sie dann auf **Weiter**.

b) Wählen Sie die Zieldomäne aus und klicken Sie auf **Weiter**.

c) Wählen Sie (falls erforderlich) eine Migrationstabelle aus und klicken Sie dann auf **Weiter**.

d) Klicken Sie auf **Fertig stellen**.

Wenn Sie die Überprüfung der Einstellungen und der Auswirkungen auf die Zieldomäne abgeschlossen haben, buchen Sie das Objekt ein und markieren Sie es als „Bereit zur Genehmigung".

Importieren von Objekten

Sie können Einstellungen nur in ausgebuchte Objekte importieren.

Gehen Sie folgendermaßen vor, um ein Objekt im Versionsüberprüfungssystem zu aktualisieren:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf ein Objekt und wählen Sie **Importieren**.
3. Wählen Sie den Speicherort und klicken Sie dann auf **Weiter**.
4. Wählen Sie die Importquelle aus.

   Sie können ein lokales Verzeichnis oder eine Netzwerkfreigabe, ein anderes Versionsüberprüfungssystem oder eine Version im aktiven Netzwerk auswählen.

   Wenn Sie ein lokales Verzeichnis oder eine Netzwerkfreigabe auswählen:

   a) Wählen Sie **Eine Sicherung auf der Festplatte** aus und klicken Sie dann auf **Weiter**.

   b) Wählen Sie ein Sicherungsverzeichnis und die Sicherung aus, die Sie importieren möchten, und klicken Sie dann auf **Weiter**.

   c) Wählen Sie (falls erforderlich) die Migrationstabelle aus und klicken Sie dann auf **Weiter**.

   d) Klicken Sie auf **Fertig stellen**.

Wenn Sie ein anderes Versionsüberprüfungssystem auswählen:

a) Wählen Sie **Ein Versionsüberprüfungssystem** aus und klicken Sie dann auf **Weiter**.

b) Wählen Sie den Versionsüberprüfungsserver und klicken Sie dann auf **Weiter**.

c) Wählen Sie das Objekt aus, das über die Einstellungen verfügt, die Sie importieren möchten, und klicken Sie dann auf **Weiter**.

d) Wählen Sie die Version des kontrollierten Objekts aus, die Sie importieren möchten, und klicken Sie dann auf **Weiter**.

e) Wählen Sie (falls erforderlich) die Migrationstabelle aus und klicken Sie dann auf **Weiter**.

f) Klicken Sie auf **Fertig stellen**.

Wenn Sie eine Version in der aktiven Umgebung auswählen:

a) Wählen Sie **Die aktive Umgebung** aus und klicken Sie dann auf **Weiter**.

b) Wählen Sie die Domäne und das Objekt mit den Einstellungen aus, die Sie importieren möchten, und klicken Sie dann auf **Weiter**.

c) Wählen Sie (falls erforderlich) die Migrationstabelle aus und klicken Sie dann auf **Weiter**.

d) Klicken Sie auf **Fertig stellen**.

4

Berichte erstellen

- Verfügbare Berichte
- Berichte über kontrollierte Objekte
- Diagnose- und Fehlerbehebungsberichte
- Bericht über aktive Objekte, die Arbeitskopie, die aktuelleste Version und Unterschiede
- Verlaufsberichte
- Arbeiten mit Berichtsordnern

Verfügbare Berichte

Sie können Berichtsvorlagen für schnelle Echtzeit-Berichterstellungszwecke sowie einfache Status-Quo-Berichte für historische Zwecke generieren. Diese Funktion ermöglicht eine schnelle Wiederherstellung von aktuellen Daten aus den Echtzeit-Berichtsvorlagen.

Berichtsvorlagen werden als XML-Dateien und historische Berichte als HTML-Dateien gespeichert.

Gehen Sie folgendermaßen vor, um eine Berichtsvorlage zu erstellen:

- Generieren Sie den Bericht und wählen Sie, die Berichtseinstellungen in einer Datei zu speichern.

  Führen Sie jetzt einfach einen Doppelklick auf die Berichtsvorlage aus, um einen aktuellen Bericht zu generieren.

Gehen Sie folgendermaßen vor, um einen historischen Bericht zu erstellen:

- Generieren Sie die Berichte und wählen Sie die Option **Speichern unter**.

  Führen Sie jetzt einen Doppelklick auf den Bericht aus, um die gespeicherte Version anzuzeigen.

Nachfolgend sind die verfügbaren Berichte aufgeführt:

- Berichte über kontrollierte Objekte
- Diagnose- und Fehlerbehebungsberichte
- Gruppenrichtlinienergebnisbericht
- Bericht über aktive Objekte, die Arbeitskopie, die aktuelleste Version und Unterschiede
- Verlaufsberichte

Berichte über kontrollierte Objekte

Sie können die folgenden Berichte erstellen:

- Einstellungsbericht
- Unterschiedsbericht
- Verlaufsbericht
- Benutzeraktivitätsbericht
- Konformitätsbericht
- Vorlagenkonfliktbericht

Gehen Sie folgendermaßen vor, um Berichte über kontrollierte Objekte zu erstellen:

1. Erweitern Sie den Knoten „Quest Group Policy Manager".
2. Klicken Sie mit der rechten Maustaste auf **Berichte** und wählen Sie dann **Neuer Bericht**.
3. Wählen Sie den zu erstellenden Berichtstyp aus.

WENN SIE ... WÄHLEN	VERFAHREN
Einstellungsbericht, Verlaufsbericht oder Konformitätsbericht	1. Klicken Sie auf **Weiter**. 2. Wählen Sie die Domäne aus, für die Sie einen Bericht erstellen möchten, und klicken Sie dann auf **Weiter**. 3. Wählen Sie das Objekt aus, für das Sie einen Bericht erstellen möchten, und klicken Sie dann auf **Weiter**. 4. Wählen Sie die Option, den Bericht zu generieren oder die Berichtseinstellungen zu speichern, und klicken Sie dann auf **Fertig stellen**.

WENN SIE ... WÄHLEN	VERFAHREN
Unterschiedsbericht	1. Klicken Sie auf **Weiter**. 2. Wählen Sie die Domäne aus, für die Sie einen Bericht erstellen möchten, und klicken Sie dann auf **Weiter**. 3. Wählen Sie die Objekte aus, für die Sie einen Bericht erstellen möchten, und klicken Sie dann auf **Weiter**. 4. Wählen Sie die Version aus, für die Sie einen Bericht erstellen möchten, und klicken Sie dann auf **Weiter**. 5. Wählen Sie, welche Einstellungen Sie in den Bericht aufnehmen möchten, und klicken Sie dann auf **Weiter**. 6. Wählen Sie die Option, den Bericht zu generieren oder die Berichtseinstellungen zu speichern, und klicken Sie dann auf **Fertig stellen**.
Benutzeraktivitätsbericht	1. Klicken Sie auf **Weiter**. 2. Wählen Sie einen Benutzer aus der Liste aus und klicken Sie dann auf **Weiter**. 3. Wählen Sie die Option, den Bericht zu generieren oder die Berichtseinstellungen zu speichern, und klicken Sie dann auf **Fertig stellen**.

WENN SIE ... WÄHLEN	VERFAHREN
Vorlagenkonfliktbericht	1. Klicken Sie auf **Weiter**. 2. Wählen Sie den Dienst aus, über den Sie einen Bericht erstellen möchten, und klicken Sie dann auf **Weiter**. 3. Klicken Sie auf **Hinzufügen**, um die Vorlagen hinzuzufügen, die Sie in den Bericht aufnehmen möchten. Positionieren Sie Kontrollkästchen neben den Vorlagen, die Sie vergleichen möchten, und klicken Sie dann auf **OK**. Die Vorlagen werden zur Listenansicht auf der Assistentenseite hinzugefügt. Mit Hilfe der Pfeile rechts im Fenster können Sie die Reihenfolge ändern, in der die Vorlagenanwendung verglichen werden kann. 4. Wenn die Liste der Vorlagen erfolgreich erstellt ist, klicken Sie auf **Weiter**. 5. Wählen Sie die Option, den Bericht zu generieren oder die Berichtseinstellungen zu speichern, und klicken Sie dann auf **Fertig stellen**.

Überprüfen auf in Konflikt stehende Vorlageneinstellungen

Group Policy Manager führt eine Überprüfung auf in Konflikt stehende Vorlageneinstellungen durch, wenn Sie ein neues Gruppenrichtlinienobjekt erstellen und Vorlagen auf dieses Objekt anwenden oder wenn Sie ein Gruppenrichtlinienobjekt auswählen, das bereits erstellt wurde, und eine Vorlage auf dieses Objekt anwenden. Wenn zwei oder mehr Vorlagen ausgewählt sind, wird ein Dialogfeld geöffnet, und Sie haben die Möglichkeit, die Überprüfung auf Konflikte zu überspringen.

Wenn Konflikte festgestellt werden, können Sie den Vorgang fortsetzen, wobei die Einstellungen der letzten Vorlage Vorrang haben. Sie können die Details der in Konflikt stehenden Einstellungen anzeigen, indem Sie auf die Schaltfläche „Details" klicken. Hierdurch wird der Vorlagenkonfliktbericht angezeigt.

Diagnose- und Fehlerbehebungsberichte

- Gruppenrichtlinienobjekt-Konsistenzbericht
- Softwareinstallationspaket-Bericht
- Bericht über verknüpfte/nicht verknüpfte Objekte
- Bericht über inaktive Richtlinieneinstellungen
- Gruppenrichtlinienobjekt-Sicherheitsbericht
- Gruppenrichtlinienergebnisse

Gehen Sie folgendermaßen vor, um Fehlerbehebungsberichte zu erstellen:

1. Erweitern Sie den Knoten „Quest Group Policy Manager".
2. Klicken Sie mit der rechten Maustaste auf **Berichte** und wählen Sie dann **Neuer Bericht**.
3. Erweitern Sie die Fehlerbehebungsberichte.

WENN SIE ... WÄHLEN	VERFAHREN
Gruppenrichtlinienobjekt-Konsistenzbericht	1. Klicken Sie auf **Weiter**. 2. Wählen Sie die Domäne aus, über die Sie einen Bericht erstellen möchten, und klicken Sie dann auf **Weiter**. 3. Wählen Sie, ob Sie die Gruppen-richtlinienobjekt acl- oder Sysvol-Dateien in den Bericht aufnehmen möchten, und klicken Sie dann auf **Weiter**. 4. Wählen Sie die Option, den Bericht zu generieren oder die Berichtsein-stellungen zu speichern, und klicken Sie dann auf **Fertig stellen**.
Softwareinstallationspaket-Bericht Bericht über verknüpfte/nicht verknüpfte Objekte Bericht über inaktive Richtlinieneinstellungen Gruppenrichtlinienobjekt-Sicherheitsbericht	1. Klicken Sie auf **Weiter**. 2. Wählen Sie die Domäne aus, über die Sie einen Bericht erstellen möchten, und klicken Sie dann auf **Weiter**. 3. Wählen Sie die Option, den Bericht zu generieren oder die Berichtsein-stellungen zu speichern, und klicken Sie dann auf **Fertig stellen**.

Gruppenrichtlinienergebnisbericht

Quest Group Policy Manager bietet eine Funktion zur Erstellung eines Berichts über die Gruppenrichtlinienergebnisse. Die Berechnung ermöglicht Ihnen, die Ergebnisse aller angewandten Gruppenrichtlinienobjekte anzuzeigen und einen Bericht hierüber zu erstellen.

Die Gruppenrichtlinienergebniseinstellungen sind abhängig von der Prioritätsstufe der angewandten Gruppenrichtlinienobjekte. Die Berichte zeigen eine Zusammenfassung der Computer- und Benutzerkonfiguration und den Endwert aller angewandten Gruppenrichtlinienobjekte an.

Um den Gruppenrichtlinienergebnisbericht erstellen zu können, muss GPMC installiert sein.

Wenn das Dienstkonto nicht über die Berechtigung zur Generierung von Gruppenrichtlinienergebnisberichten verfügt, werden im Berichtsassistenten verschiedene Fehler angezeigt. Um die Gruppenrichtlinienergebnisberichte für einen Benutzer oder Computer richtig zu generieren, muss das Dienstkonto über die Berechtigung zum Lesen von Gruppenrichtlinienergebnisdaten für die Domäne oder Organisationseinheit verfügen, die den Benutzer oder Computer enthält, oder das Dienstkonto muss ein Mitglied einer lokalen Administratorengruppe auf dem Zielcomputer sein.

Gehen Sie folgendermaßen vor, um einen Gruppenrichtlinienergebnisbericht zu erstellen:

1. Erweitern Sie den Knoten „Quest Group Policy Manager".
2. Klicken Sie mit der rechten Maustaste auf **Berichte** und wählen Sie dann **Neuer Bericht**.
3. Wählen Sie den Gruppenrichtlinienbericht.
4. Wählen Sie die Domäne aus, über die Sie einen Bericht erstellen möchten, und klicken Sie dann auf **Weiter**.
5. Um die Computereinstellungen aufzunehmen, wählen Sie Ihren lokalen Computer aus.

   – ODER –

   Klicken Sie auf **Durchsuchen**, um einen Computer im Netzwerk anzugeben. Geben Sie die erforderlichen Suchinformationen ein, klicken Sie auf **OK** und dann auf **Weiter**.

Computer müssen kompatibel sein. (Zum Beispiel Windows XP und Server 2003. Server 2000 ist nicht mit den GPMC-Ergebnissen kompatibel.)

   Wenn Sie die Computereinstellungen nicht in den Bericht aufnehmen möchten, aktivieren Sie das Kontrollkästchen „Keine Richtlinieneinstellungen für den ausgewählten Computer im Ergebnis anzeigen (nur Benutzerrichtlinieneinstellungen anzeigen)".

6. Wählen Sie den Benutzer aus, dessen Einstellungen Sie anzeigen möchten, und klicken Sie dann auf **Weiter**.

   Wenn Sie die Benutzerrichtlinieneinstellungen nicht in den Bericht aufnehmen möchten, aktivieren Sie das Kontrollkästchen „Keine Benutzerrichtlinieneinstellungen im Ergebnis anzeigen (nur Computerrichtlinieneinstellungen)".

7. Wählen Sie die Option, den Bericht zu generieren oder die Berichtseinstellungen zu speichern, und klicken Sie dann auf **Fertig stellen**.

Bericht über aktive Objekte, die Arbeitskopie, die aktuelleste Version und Unterschiede

Gehen Sie folgendermaßen vor, um einen Bericht zu erstellen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf das kontrollierte Objekt und wählen Sie **Berichte**.
    - Um einen Bericht über die Einstellungen des aktiven kontrollierten Objekts zu erstellen, wählen Sie **Aktiv**.
    - Um einen Bericht über die Einstellungen ausgebuchter Objekte und der Arbeitskopie zu erstellen, klicken Sie auf **Arbeitskopie**.
    - Um einen Bericht über die aktuellste Version des kontrollierten Objekts in der Versionsüberprüfung zu erstellen, klicken Sie auf **Letzte**.
    - Um einen Bericht zu erstellen, der die Unterschiede zwischen den Einstellungen angibt, klicken Sie auf **Unterschiede**.

Um einen Bericht zu erstellen, der die Unterschiede zwischen zwei Objekten anzeigt, wählen Sie die Objekte aus, klicken Sie mit der rechten Maustaste und wählen Sie „Unterschiede".

3. Zeigen Sie den Bericht an.

    – ODER –

    Klicken Sie auf **Drucken**, um den Bericht zu drucken.

    – ODER –

    Klicken Sie auf **Speichern unter**, um den Bericht als eine HTML-Datei zu speichern.

    Um den Bericht zu einem späteren Zeitpunkt anzuzeigen, wählen Sie den entsprechenden Bericht aus und doppelklicken Sie darauf, um den anzuzeigenden Bereich zu erweitern.

4. Klicken Sie auf **Schließen**.

Verlaufsberichte

Gehen Sie folgendermaßen vor, um einen Bericht zu erstellen:

1. Erweitern Sie den Knoten „Versionsüberprüfungs-Root" und wählen Sie den erforderlichen Container aus.
2. Klicken Sie mit der rechten Maustaste auf das kontrollierte Objekt und wählen Sie **Verlauf anzeigen**.
3. Um die Einstellungen einer früheren Version anzuzeigen, wählen Sie die Version aus und klicken dann auf **Ansicht**.
4. Um die Unterschiede zwischen den Einstellungen verschiedener Versionen anzuzeigen, wählen Sie die entsprechenden Versionen aus und klicken dann auf **Unterschiede**.
5. Um die Einstellungen einer früheren Version zu holen, wählen Sie die entsprechende Version aus und klicken dann auf **Download von**.

Das kontrollierte Objekt muss ausgebucht sein, um die Funktion „Holen" nutzen zu können.

6. Zeigen Sie den Bericht an.

   – ODER –

   Klicken Sie auf **Drucken**, um den Bericht zu drucken.

   – ODER –

   Klicken Sie auf **Speichern unter**, um den Bericht als eine HTML-Datei zu speichern.

7. Klicken Sie auf **Schließen**.

   Um den Bericht zu einem späteren Zeitpunkt anzuzeigen, wählen Sie den entsprechenden Bericht aus und doppelklicken Sie darauf, um den anzuzeigenden Bereich zu erweitern.

Arbeiten mit Berichtsordnern

„Berichte" im Quest Group Policy Manager spiegelt die Inhalte des Ordners „Eigene Quest Group Policy Manager-Berichte" im Verzeichnis „Eigene Dokumente" wider.

Gehen Sie folgendermaßen vor, um einen neuen Ordner zu erstellen:

- Klicken Sie mit der rechten Maustaste auf **Berichte** oder einen beliebigen Unterordner und wählen Sie **Neu | Ordner**.

Gehen Sie folgendermaßen vor, um einen Ordner umzubenennen:

- Klicken Sie mit der rechten Maustaste auf einen beliebigen Unterordner unter „Berichte" und geben Sie den neuen Namen ein.

Der Name muss ein gültiger Windows-Dateiname sein und darf nicht in Konflikt mit anderen Ordnernamen desselben übergeordneten Ordners stehen.

Gehen Sie folgendermaßen vor, um einen Ordner zu löschen:

1. Klicken Sie mit der rechten Maustaste auf einen beliebigen Unterordner unter „Berichte" und wählen Sie **Löschen**.
2. Bestätigen Sie Ihre Auswahl.

Gehen Sie folgendermaßen vor, um einen Ordner oder Bericht zu verschieben:

- Wählen Sie den Ordner oder Bericht aus und verschieben Sie ihn per Drag & Drop an seine neue Position.

Sie können einen Bericht nicht in den Ordner verschieben, in dem er sich aktuell befindet.
Sie können einen Ordner nicht in seinen direkt übergeordneten Ordner verschieben.

Gehen Sie folgendermaßen vor, um Berichte mit Hilfe von Windows Explorer zu verwalten:

1. Klicken Sie mit der rechten Maustaste auf **Berichte** und wählen Sie dann **Ordner im Explorer öffnen**.

   Hier können Sie Ihre Dateien auf gewohnte Weise verwalten.

2. Wenn Sie zu Quest Group Policy Manager zurückkehren, klicken Sie mit der rechten Maustaste auf **Berichte** und wählen Sie **Aktualisieren**, um zu gewährleisten, dass Ihre Ansicht aktualisiert wird.

5

Arbeiten mit Quest ADM-Editor

- Arbeiten mit .adm-Dateien
- Erstellen und Bearbeiten von .adm-Dateien
- Anpassen der ADM-Editoranzeige

Arbeiten mit .adm-Dateien

Die Arbeit mit registrierungsbasierten Gruppenrichtlinien wird durch die Verwendung von administrativen Vorlagedateien (.adm) etwas vereinfacht. Die .adm-Dateien legen fest, welche Gruppenrichtlinienobjekteinstellungen unter dem Ordner „Administrative Vorlage" für die Benutzer- und Computerkonfiguration angezeigt werden.

Die .adm-Datei ist eine Vorlage, die die administrative Schnittstelle definiert, die während der Bearbeitung eines Gruppenrichtlinienobjekts verfügbar ist. Auf die für die Erstellung und Bearbeitung von .adm-Dateien erforderlichen Daten kann einfach mit Hilfe des Quest ADM-Editors zugegriffen werden. Nachfolgend ist der Inhalt einer .adm-Datei aufgeführt:

- Speicherposition der Registrierung
- Optionen für jede Einstellung
- Eingabeverfahren für Parameter
- Anzuzeigender Standardwert
- Beschreibungen der Einstellungen auf der Registerkarte „Erklärung"
- Von jeder Windows-Version unterstützte Einstellungen

Alle in Group Policy Manager-Vorlagen verwendeten ADM-Dateien müssen dem Unicode-Format entsprechen.

Erstellen und Bearbeiten von .adm-Dateien

Der Quest ADM-Editor ist in QGPM enthalten. Mit diesem Hilfsprogramm können Sie .adm-Dateien mit Hilfe einer benutzerfreundlichen Schnittstelle erstellen und bearbeiten.

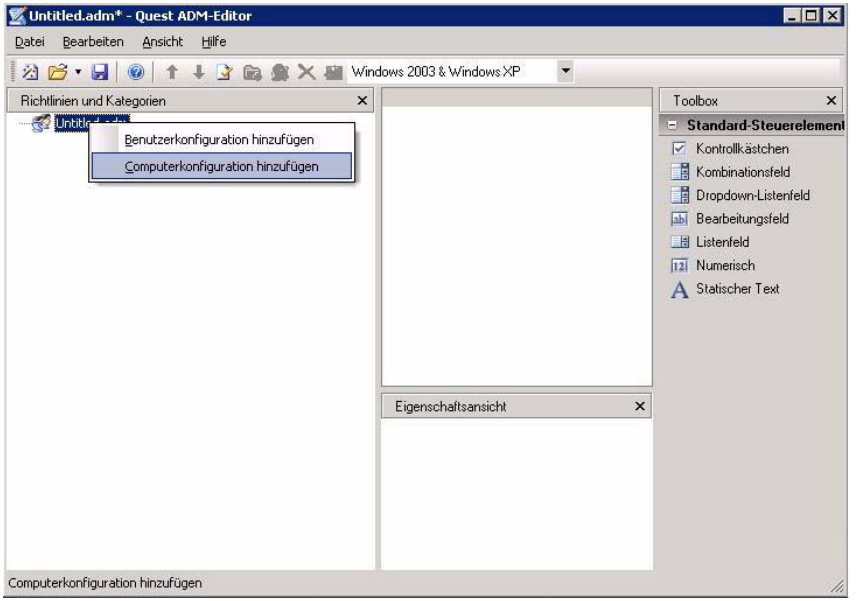
Gehen Sie folgendermaßen vor, um eine .adm-Datei zu erstellen:

1. Wählen Sie im Quest Group Policy Manager-Container die Option **ADM-Editor** aus.
2. Wählen Sie **Datei | Neu**.
3. Klicken Sie auf **Weiter** im Assistenten für eine neue ADM-Datei.
4. Wählen Sie den Dateityp, den Sie erstellen möchten, und klicken Sie dann auf **Weiter**.

   In diesem Arbeitsschritt wird eine leere .adm-Datei erstellt. Wenn Sie Benutzer, Computer oder Benutzer und Computer auswählen, wird der zugehörige Ordner „Administrative Vorlage" automatisch zur Datei hinzugefügt.
5. Klicken Sie auf **Fertig stellen**.

   Eine neue ADM-Datei wird erstellt.

6. Klicken Sie mit der rechten Maustaste auf die .adm-Datei und wählen Sie **Benutzerkonfiguration hinzufügen** oder **Computer-konfiguration hinzufügen** oder beide Optionen aus.



Der Container „Administrative Vorlagen" wird angezeigt.

7. Klicken Sie mit der rechten Maustaste auf **Administrative Vorlage** und wählen Sie **Kategorie hinzufügen**.
8. Geben Sie einen Namen für die Kategorie ein.
9. Klicken Sie mit der rechten Maustaste auf die Kategorie und wählen Sie **Richtlinie hinzufügen**.
10. Geben Sie einen Namen für die Richtlinie ein.

    Sie können jetzt die Richtlinie so konfigurieren, dass sie die erforderlichen Einstellungen enthält, indem Sie Steuerelemente hinzufügen und die Eigenschaften bearbeiten.

11. Fügen Sie ein Steuerelement hinzu, indem Sie einen Doppelklick auf die gewünschte Option in der Toolbox ausführen und ihre Eigenschaften bearbeiten.

    – ODER –

    Klicken Sie mit der rechten Maustaste auf die Richtlinie und führen Sie die Schritte des Assistenten für neue Teile durch, um vordefinierte Teile für die Bearbeitung hinzuzufügen.

12. Geben Sie einen Namen für die .adm-Datei ein und wählen Sie **Speichern**.

    Sie können die .adm-Datei jetzt zu den Gruppenrichtlinienvorlagen hinzufügen.

Gehen Sie folgendermaßen vor, um eine .adm-Datei zu bearbeiten:

1. Wählen Sie im Quest Group Policy Manager-Container die Option **ADM-Editor** aus.
2. Wählen Sie **Datei | Öffnen** und wählen Sie dann eine zuvor gespeicherte .adm-Datei.
3. Bearbeiten Sie die Datei wie gewünscht.

   Sie können eine Kategorie hinzufügen, eine Richtlinie hinzufügen oder vorhandene Richtlinien und Kategorien entfernen.

4. Wählen Sie **Datei | Speichern**.

Sie können eine neue oder vorhandene Datei überprüfen, um zu gewährleisten, dass diese ordnungsgemäß erstellt wurde, indem Sie entweder auf Datei prüfen klicken oder F7 drücken.

Mit dem ADM-Editor erstellte .adm-Beispieldatei

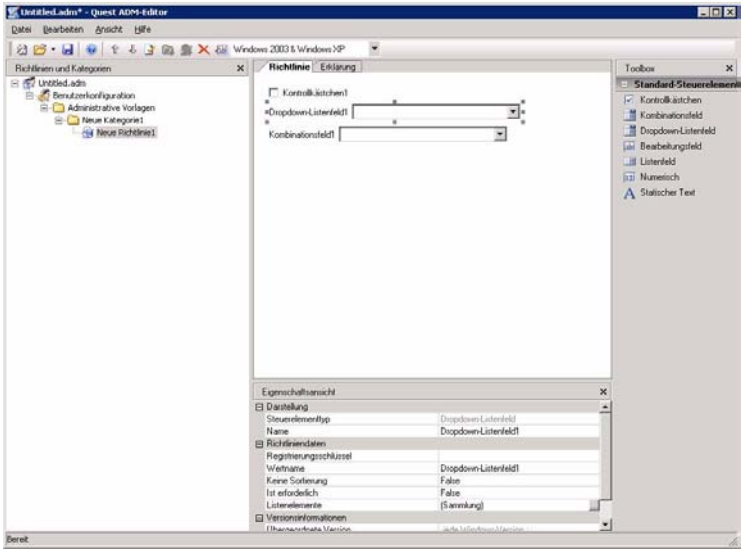
Dieses Beispiel zeigt, wie die folgende ADM-Datei für die Definition der Konfiguration verschiedener Internet Explorer-Einstellungen mit Hilfe des ADM-Editors erstellt wird:

```
CLASS USER
CATEGORY „Erweiterte Einstellungen“
    POLICY „Suchen“
        KEYNAME „Software\Microsoft\Internet Explorer\Main“
        PART „Provider-Schlüsselwort eingeben (geben Sie INTRANET
ein, wenn Sie über einen internen AutoSearch-Server verfügen):“
EDITTEXT
            VALUENAME „Provider“
           KEYNAME „Software\Microsoft\Internet Explorer\SearchURL“
        END PART
        PART „Bei Suche mittels Adressleiste:“ DROPDOWNLIST
            VALUENAME „AutoSearch“
            ITEMLIST
               NAME „Ergebnisse anzeigen und Seite mit der höchsten
Trefferquote aufrufen“ VALUE NUMERIC 3 DEFAULT
                NAME „Nur die Seite mit der höchsten Trefferquote
aufrufen“ VALUE NUMERIC 2
                NAME „Nur die Ergebnisse im Hauptfenster anzeigen“
VALUE NUMERIC 1
                NAME „Nicht mittels der Adressleiste suchen“ VALUE
NUMERIC 0
            END ITEMLIST
        END PART
    END POLICY
END CATEGORY ;Erweiterte Einstellungen
```

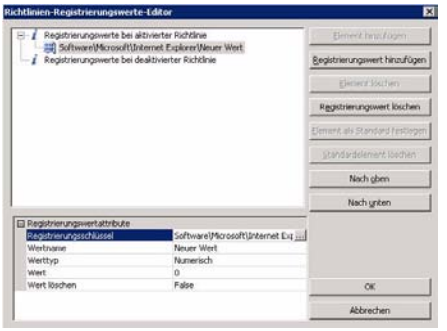
Gehen Sie folgendermaßen vor, um diese .adm-Datei zu erstellen:

1. Wählen Sie im Quest Group Policy Manager-Container die Option **ADM-Editor** aus.
2. Wählen Sie **Datei | Neu**.
3. Klicken Sie auf **Weiter** im Assistenten für eine neue ADM-Datei, um den Vorgang zu starten.
4. Wählen Sie **Benutzer** aus und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf **Fertig stellen**.
6. Klicken Sie mit der rechten Maustaste auf **Administrative Vorlage** und wählen Sie **Kategorie hinzufügen**.
7. Geben Sie **Erweiterte Einstellungen** als den Namen für die Kategorie ein.

8. Klicken Sie mit der rechten Maustaste auf die Kategorie und wählen Sie **Richtlinie hinzufügen**.
9. Geben Sie **Sicherheit** als den Namen für die Richtlinie ein.
10. Fügen Sie ein Dropdown-Listenfeld hinzu.



11. Wählen Sie das Dropdown-Listenfeld, wählen Sie die Listenelement-eigenschaft (in der Eigenschaftsansicht), klicken Sie auf die Schaltfläche **Durchsuchen** und fügen Sie Elemente im Listenelementeditor hinzu.
12. Fügen Sie einen zusätzlichen Wert zum Element (Vorgangsliste) hinzu, indem Sie auf **Registrierungswert hinzufügen** klicken.



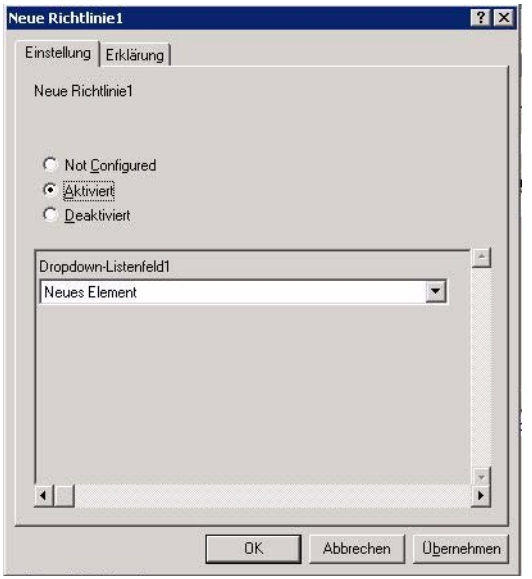
13. Wenn Sie alle erforderlichen Änderungen vorgenommen haben, klicken Sie auf **OK**.

14. Geben Sie einen Namen für die .adm-Datei ein und wählen Sie **Speichern**.

Das Dropdown-Listenfeld hat nun das folgende Format:

```
PART „Bei Suche mittels Adressleiste:“ DROPDOWNLIST
        VALUENAME „AutoSearch“
        ITEMLIST
              NAME „Ergebnisse anzeigen und Seite mit der höchsten
Trefferquote aufrufen“ VALUE NUMERIC 3 DEFAULT
                 ACTIONLIST
                    KEYNAME „Software\Microsoft\Internet Explorer\Main“
                    VALUENAME „Zusätzlicher Wert“ VALUE NUMERIC 0
                   VALUENAME „Zusätzlicher Zeichenkettenwert“ VALUE „etwas“
                 END ACTIONLIST
              NAME „Nur die Seite mit der höchsten Trefferquote aufrufen“
VALUE NUMERIC 2
              NAME „Nur die Ergebnisse im Hauptfenster anzeigen“ VALUE
NUMERIC 1
              NAME „Nicht mittels der Adressleiste suchen“ VALUE NUMERIC 0
        END ITEMLIST
END PART
```

Die fertig gestellte Datei wird wie folgt angezeigt:

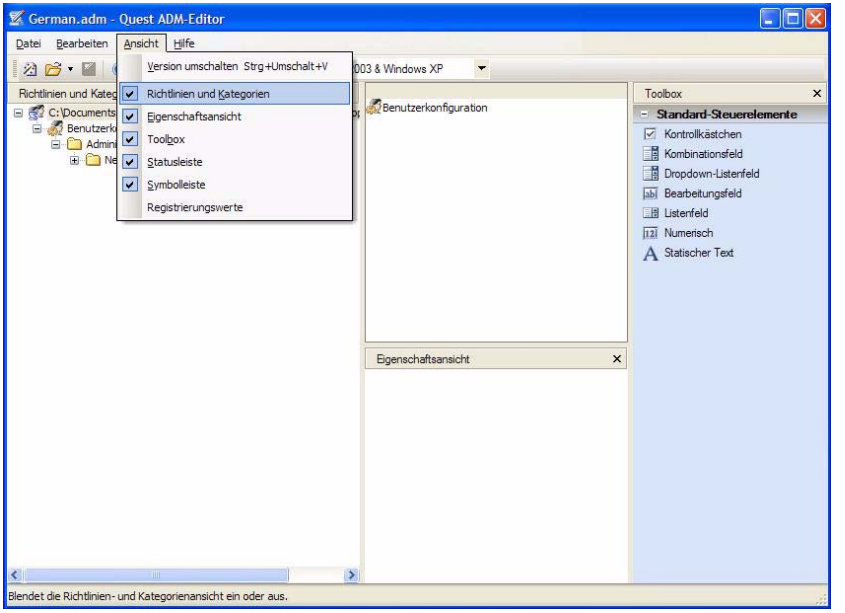


Anpassen der ADM-Editoranzeige

Sie können den ADM-Editor so anpassen, dass er eine beliebige Kombination der folgenden Elemente anzeigt: Richtlinien und Kategorien, Eigenschaftsansicht, Toolbox, Statusleiste, Symbolleiste und Registrierungswerte.

Gehen Sie folgendermaßen vor, um die Anzeigen zu verändern:

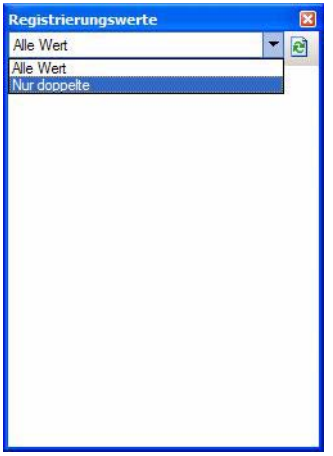
1. Wählen Sie im Quest Group Policy Manager-Container die Option **ADM-Editor** aus.
2. Klicken Sie auf **Ansicht**.



3. Aktivieren oder deaktivieren Sie die Optionen Ihren Wünschen entsprechend.

4. Wenn Sie **Registrierungswerte** auswählen, wenn Ihre Datei fertig gestellt ist, wird eine Strukturansicht der Richtlinie, so wie diese in der Registrierung angewandt würde, angezeigt.

Von hier aus können Sie auch nach Duplikaten in der Datei suchen, indem Sie „Nur doppelte" aus der Liste auswählen.



Glossar

Dieses Glossar enthält Definitionen aus Microsoft-Publikationen.

A

Active Directory
Der Windows 2000/2003 Verzeichnisdienst.

Administratorrechte
Administratorrechte sind die Rechte, die einem Mitglied der lokalen Administratorgruppe gewährt werden. Dieses Mitglied kann Aktionen wie etwa die Erstellung von Benutzerkonten, die Erstellung von Gruppen und das Hinzufügen von Gruppenmitgliedern durchführen.

Aktives Gruppenrichtlinienobjekt
Aktive Gruppenrichtlinienobjekte sind die Gruppenrichtlinienobjekte, die in der Unternehmensumgebung vorhanden sind und die Benutzer und Computereinstellungen beeinflussen.

Authentifizierung
Der für die lokale Anmeldung bei einem Computer erforderliche Prozess. Die Authentifizierung erfordert einen gültigen Benutzernamen und ein Kennwort, der bzw. das in der lokalen Kontodatenbank vorhanden ist. Es wird ein Zugriffs-Token erstellt, wenn die gelieferten Informationen mit dem Konto in der Datenbank übereinstimmen.

B

Berechtigung
Eine mit einem Objekt verbundene Regel, um den Zugriff auf ein bestimmtes Objekt im Netzwerk zu regeln. Ein Benutzer kann beispielsweise über einen Lese- und Schreibzugriff auf eine Datei im Netzwerk verfügen.

D

Distinguished Name (DN)

Der Distinguished Name ist der vollständig qualifizierte Name eines Objekts in einem hierarchischen System. Distinguished Names werden für alle Active Directory-Objekte und im Domain Name System (DNS) verwendet. Es dürfen keine zwei Objekte in diesen Systemen denselben Distinguished Name haben.

Domäne

Eine Domäne (in Relation zu einem Microsoft-Netzwerk) ist eine logische Zusammenfassung von Ressourcen, die aus Computern, Druckern, Computerkonten, Benutzerkonten und anderen zugehörigen Objekten besteht. Die Domäne hat außerdem ein System zur Authentifizierung von Benutzerkonten und Computerkonten.

Domänencontroller

Ein Server, der die Kennwörter zur Anmeldung bei der Domäne authentifiziert und die Sicherheitsrichtlinie und die Sicherheitskonten-Masterdatenbank für eine Domäne pflegt.

G

Gesamtstruktur

Eine oder mehrere Domänenstrukturen, die keinen zusammenhängenden Namespace bilden, jedoch ein gemeinsames Schema, eine gemeinsame Konfiguration und einen globalen Katalog nutzen.

Gruppe

Eine Gruppe (in Relation zu einem Microsoft-Netzwerk) ist eine logische Zusammenfassung von Benutzerkonten oder anderen Gruppen. Zusammenfassung von Benutzern, Computern, Kontakten und anderen Gruppen.

Gruppenrichtlinienobjekt

Ein Gruppenrichtlinienobjekt ist die Gruppierung von Richtlinieneinstellungen für Benutzer und Computer.

K

Knoten

In einem Netzwerk ist ein Knoten ein Verbindungspunkt, d. h. entweder ein Verteilerpunkt oder ein Endpunkt für die Datenübertragungen.

O

Objekt

Ein Objekt ist eine Windows NT-Einheit. Als Beispiel sind hier Benutzer, Gruppen und Computer aufgeführt. Die Zugriffsrechte auf das Objekt umfassen die Erstellung, das Lesen, das Bearbeiten und das Löschen.

Organisationseinheit

Organisationseinheit
Eine Organisationseinheit ist ein Containerobjekt, das verwendet wird, um die Active Directory-Objekte innerhalb einer Domäne logisch zu organisieren.

R

Richtlinie

Allgemeine Kontrollen, die die Sicherheit einer Betriebsumgebung erhöhen. In Windows 2000 beeinflussen Richtlinien die Einschränkungen hinsichtlich der Verwendung von Kennwörtern und der Zuweisung von Rechten und legen die Ereignisse fest, die im Sicherheitsprotokoll verzeichnet werden.

Rollback

Ausgehend vom Konformitätsassistenten können die Benutzer innerhalb des Versionsüberprüfungssystems einen Rollback zu jedem beliebigen Punkt im Verlauf des Gruppenrichtlinienobjekts durchführen.

S

Schema

Die Metadaten, die die Verwendung von Objekten innerhalb einer bestimmten Struktur beschreiben.

Sites

Eine Zusammenfassung von Domänencontrollern. Sites werden durch das Teilnetz eines Domänencontrollers definiert.

SLA

Softwarelizenzabkommen

Z

Zurückweisen

Wenn die Bearbeitung eines Gruppenrichtlinienobjekts zurückgewiesen wird, werden keine Änderungen übernommen, und der Gruppenrichtlinienobjektstatus wird in den Status „Verfügbar" zurückgesetzt.

INDEX

A
ADM-Dateien 38
ADM-Editor 99
Änderungen
  Genehmigen oder zurückweisen 69, 70
Anschlussanforderungen 25
Anstehende Genehmigung 66
Anwenden von Vorlagen 77
Anzeigen
  Eigenschaften 57
  Unterschiede zwischen Versionen 58
Anzeigen des Verlaufs 56
Ausbuchung rückgängig machen 62
Ausgebuchte Objekte 62

B
Bearbeitungen genehmigen 69, 70
Bearbeitungen zurückweisen 69
Benachrichtigungssystem 32
Bereitstellung planen 69
Berichte 86
  Gruppenrichtlinienergebnis 92
  Unterschiede anzeigen 58
Bezeichnen eines Containers 45
Bezeichnungen 55

C
Containereigenschaften 46
Containerhierarchie 45

E
Einstellungen deaktivieren 75
Erstellen
  ADM-Dateien 99
  Bezeichnungen 55
  Gruppenrichtlinienobjekt 49
  Rolle 30
  Vorlagen 53
  Vorlagen von registrierten Gruppenrichtlinienobjekten 54

G
Genehmigung anfordern 61
Genehmigung auf mehreren Ebenen 67
Genehmigung zurückziehen 64

I
Importieren der INF-Dateieinstellungen 80
Importieren von Einstellungen 83

K
Konfigurieren
  Benachrichtigung 32
  Rollenbasierte Delegation 28
  Versionsüberprüfungsserver 22
Konformität 71
Kopieren und Einfügen 47

L
Lizenzoptionen 27
Löschen von Objekten 61

O
Objekte ausbuchen 60
Objekte bearbeiten 74
Objekte einbuchen 63

P
Protokollierungsoptionen 27

R
Registrieren von Objekten 40
Registriertes Objekt 55
Rollen
  Benutzer 29
  Genehmiger 29
  Moderator 29
  Systemadministrator 28
Rollen delegieren 31
Rollenbasierte Delegation 28

S
Status
  Anstehende Bereitstellung 66
  Ausgebucht 62
  Registriert 55
  Verfügbar 59

V

Verfügbare Objekte 59
Vorige Version wiederherstellen 65
Vorlage
  Anwenden 77
  Bearbeiten 80
  Benutzerdefinierte ADM-Dateien 38
  Erstellen 53
  Erstellen von registrierten
    Gruppenrichtlinienobjekten 54